
GREd Web 改ざんチェック Cloud ユーザーガイド

第 15 版

(2024 年 4 月 1 日)



変更履歴

Version	日付	備考
8	2020/5/20	V3.8 対応
9	2022/2/28	V3.11 対応
10	2022/5/31	機能変更対応
11	2022/8/1	GUI リニューアル対応
12	2022/9/1	V3.12 対応
13	2023/4/5	V3.13 対応
13.1	2023/6/2	V3.13.1 対応
14	2023/9/29	V3.14 対応
15	2024/4/1	V3.15 対応

目次

1.	はじめに.....	5
2.	GREd Web 改ざんチェック Cloud サービス概要.....	5
2.1	検知可能な改ざん.....	5
2.2	改ざんを発見した場合.....	5
2.3	改ざん検知時のページ切り替え.....	6
3.	管理コンソールの見方、使い方.....	7
3.1	ログイン・ログアウト.....	7
3.2	ダッシュボード画面.....	9
3.3	解析結果表示 緑 (SAFE・安全).....	11
3.4	解析結果表示 赤 (DANGER・危険).....	12
3.5	解析結果表示 黄色 (Warning・警告) クロスドメインスクリプト検知 15	
3.6	解析結果表示 黄色 (Warning・警告) TOP ページの見た目変化検知	16
3.7	解析結果表示 黄色 (Warning・警告) タグ・JavaScript の変化検知	17
3.8	解析結果表示 黄色 (Warning・警告) EXE 解析検知.....	18
3.9	改ざん検知時のメール送信.....	19
3.10	お知らせ機能.....	20
4.	解析履歴.....	21
4.1	解析履歴.....	21
4.2	レポート作成.....	22
4.3	週間レポートメール.....	23
5.	各種設定.....	24
5.1	ユーザー管理.....	24
5.2	ユーザー情報の確認・変更.....	25
5.3	パスワードの変更.....	28
5.4	除外 URL の登録.....	29
5.5	ホワイトリストの登録.....	31
5.6	監視の ON/OFF とウェブ解析対象階層の指定.....	33
5.7	クロスドメインの許可設定.....	34
5.8	改ざん検知時のページ切り替え機能の設定.....	37
5.9	GREd 証明書の設定.....	39
5.10	非リンク URL の登録.....	41
6.	その他の機能・サービス.....	43
6.1	解析サイトの検索.....	43
6.2	オンデマンドチェック機能.....	44
6.3	GREd 証明書.....	45

6.4	ポートスキャン診断機能	46
6.5	Joomla 簡易脆弱性診断機能.....	49
6.6	リンク切れ検知機能	52
6.7	リンク構造可視化機能.....	55
6.8	全サイトの状態	59
6.9	一括ダウンロード.....	60
6.10	パスワードをお忘れの場合.....	62
6.11	ログイン履歴確認機能.....	62
7.	申込み（新規申込・変更申請）	63
7.11	新規申込	63
7.12	解析する URL 数、解析対象ホスト数.....	63
7.13	解析する URL の絞り込み(除外 URL の登録)	63
7.14	解析する URL の絞り込み(ウェブ解析対象階層の指定).....	64
7.15	変更申請	64
付録	新規申込書	65
付録	変更申請書	66
付録	解約申請書	67
付録	管理画面 URL.....	68
付録	アラートメールサンプル	69

1. はじめに

本書は、「GREd Web 改ざんチェック Cloud」の導入のための手順と、導入後の設定や機能について解説しております。不明点がございましたら、以下までご連絡をお願いします。
[問い合わせフォーム](https://www.securebrain.co.jp/form/gredss/sbformmail.php)

<https://www.securebrain.co.jp/form/gredss/sbformmail.php>


2. GREd Web 改ざんチェック Cloud サービス概要

「GREd Web 改ざんチェック Cloud」は、お客様の Web サイトが改ざんの被害にあっていないかを定期的に確認するサービスです。監視対象となる URL を登録するだけで、日立システムズのシステムが自動的にリンクを辿り、各ページの解析を行います。改ざん発見時には、アラート送信と詳細なレポートを生成する機能を提供します。

2.1 検知可能な改ざん

- ・サイバー攻撃等による Web サイトの改ざん
- ・脆弱性を悪用した攻撃を行う Web サイトへの改ざん
- ・ウイルスなどが自動的にダウンロードされる Web サイトへの改ざん
- ・政治意思や思想を誇示するために意図的にページを書き換える改ざん
- ・ドライブバイダウンロード攻撃の踏み台に利用するための Web 改ざん
- ・SEO ポイズニングによる Web 改ざん

2.2 改ざんを発見した場合

改ざんを発見した場合、管理者にアラートメールを送信します。詳細はそのメールに記載されている URL をクリックするか、管理コンソールトップページのカレンダーの赤い  のアイコンをクリックすると確認いただけます。



■ 詳細レポート

詳細レポートには、改ざんを検知した URL、改ざんの種類とその説明、悪質コードの脅威名とソースを表示します。このレポートにより、迅速な対応が可能になります。

問題が見つかりました

2022年5月13日 15:29

改ざんを検知したページのURL

改ざんの種類と説明

より詳しい情報を表示 (ソースコードを表示)

検知箇所をリンク構造で表示

2.3 改ざん検知時のページ切り替え

改ざんが見つかった場合、自動で安全なページ（GREED 内のメンテナンスページ）に切り替えることができます。この改ざん検知時のページ切り替え機能を設定しておくことで、お客様の Web サイトが復旧するまで、エンドユーザーへの被害を防ぐことができます。この機能は、お客様の Web サイトが安全な状態になると表示されません。

【メンテナンス画面】



3. 管理コンソールの見方、使い方

各種設定、サービスの提供は、管理コンソールより行います。

3.1 ログイン・ログアウト

ログイン

管理画面 URL にアクセスし、ログイン画面に、ID とパスワードを入力し、「ログインする」をクリックします。

初めて管理コンソールにログインするには、お客様にてパスワードを設定する必要があります。サービス開始後に送付される登録通知メールの手順に従い、パスワードを設定してください。パスワード設定後、パスワード設定完了の通知が届きますので、メールに記載しているログイン画面 URL よりログインして下さい。

A screenshot of the login form. It features two input fields: 'ユーザーID' (User ID) and 'パスワード' (Password). Below the fields is a blue button labeled 'ログインする' (Login) with a right-pointing arrow icon. Underneath the button is a link that says 'パスワードをお忘れの場合' (If you forgot your password).

システムメンテナンスや障害の詳細情報はログイン後に確認いただけます。詳細は「3.10 お知らせ機能」を参照してください。

二要素認証

二要素認証を有効に設定することでIDとパスワードでの認証後にワンタイムパスワードを使用した二要素認証をします。スマートフォンにインストールした認証アプリからワンタイムパスワードを取得することでログインしてください。認証アプリは Google Authenticator または Microsoft Authenticator を利用してください。二要素認証の設定方法については「5.2 ユーザー情報の確認・変更」を参照してください。



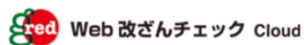
二要素認証

認証アプリからワンタイムパスワードを取得して認証してください。
ワンタイムパスワードを取得できない場合は、ログイン画面の「パスワードをお忘れの場合」からパスワードを再発行して二要素認証を無効にしてください。

認証

ログアウト

ヘッダーの右上にある『ログアウト』ボタンをクリックすると、ログアウトされます。



全サイト操作 ユーザー情報



ログアウト

3.2 ダッシュボード画面

正しくログインが完了すると、ダッシュボード画面へ遷移します。ダッシュボード画面では、最新の解析結果と過去の解析結果の統計情報（直近、ウィークリー、マンスリー）の棒グラフと解析履歴（1年分）をカレンダーで表示します。



項目名	内容
① 最終結果	最新の解析結果を表示します。詳細は 3.3 以降の「解析結果表示」参照して下さい。
② 本日の解析結果履歴	最新の解析結果を表示します。
③ 直近の解析結果	直近の 8 回分の解析結果（解析毎の検知数の累計）を棒グラフで表示します。
④ ウィークリーの解析結果	今週を含めて 8 週間分の解析結果の累計を一週間ごとの棒グラフで表示します。
⑤ マンスリーの解析結果	今月を含めて 8 か月分解析結果の累計を一か月ごとの棒グラフで表示します。
⑥ 解析結果カレンダー	解析の結果を、それぞれ安全、警告、危険のマークをカレンダー上に表示します。カレンダー上部の「期間を選択」リストボックスで表示する年月の切り替えが出来ます。
⑦ 解析サイトリスト	解析サイトが複数ある場合にはリストで表示されます。リストボックスに表示される解析サイトを選択すると表示対象の解析サイトの切り替えが出来ます。
⑧ 詳細設定ボタン	各解析サイトの解析履歴、詳細設定画面に遷移します。

⑨	ツールチップ	<p>各棒グラフにカーソルを合わせると解析結果の検知数が表示されます。</p> <p>改ざん検知された場合</p>  <p>改ざん検知が無い場合</p> 
⑩	ログイン履歴	<p>前回のログイン日時を表示します。右側の「履歴」をクリックすると過去のログイン履歴を表示するページに遷移します。詳細は 6.11 の「ログイン履歴確認機能」を参照して下さい。</p>
⑪	お知らせ	<p>管理画面には最新のお知らせが表示されます。「一覧を見る」をクリックすると過去のお知らせを確認することができます。詳細は 3.10 の「お知らせ機能」を参照してください。</p>

※アイコンと棒グラフの色について

(詳細は 3.3 以降の「解析結果表示」参照して下さい。)



3.3 解析結果表示 緑 (SAFE・安全)


解析した結果、安全なサイトであると判定された場合、画面には「SAFE」と緑で表示されます。

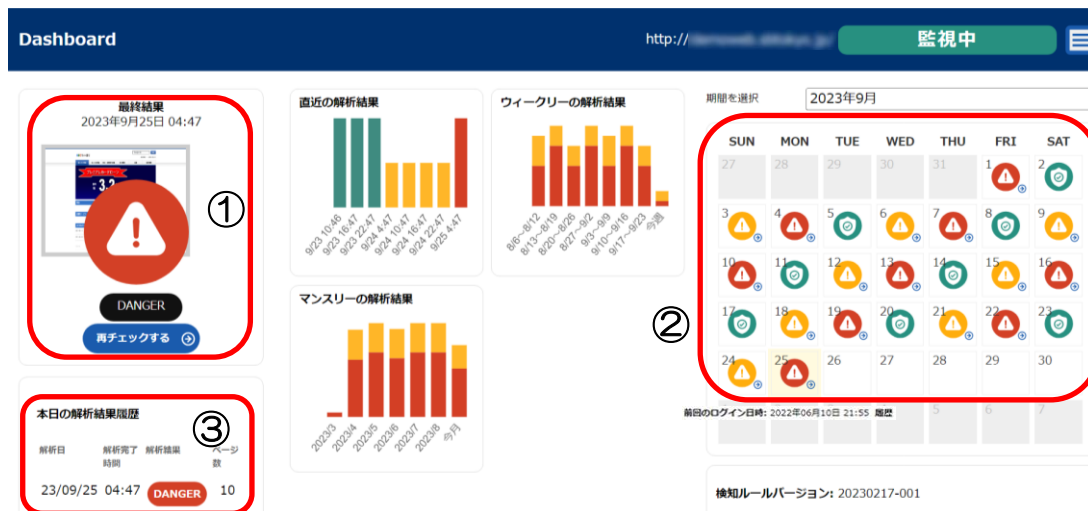


「SAFE」表示内容




	項目名	内容
①	判定結果	安全なサイトであることを示す「SAFE」が表示されます。
②	解析結果カレンダー	解析の結果、安全なサイトと判断された場合には緑色の🟢マークをカレンダー上に表示します。


3.4 解析結果表示 赤 (DANGER・危険)

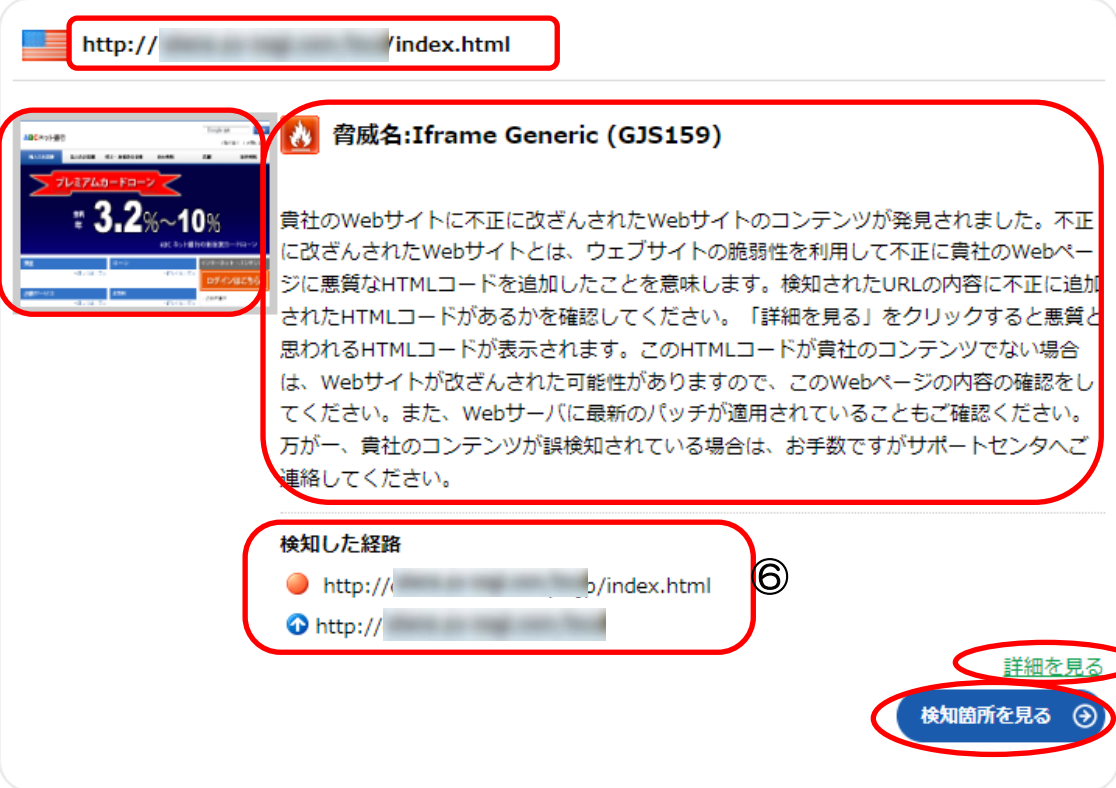
解析を行った結果、危険なサイトであると判定された場合、画面には赤の  マークが表示されます。




「DANGER」表示内容

項目名	内容
① 判定結果	危険なサイトであることを示す赤い  が表示されます。
② 解析結果カレンダー	解析の結果、危険なサイトと判断された場合には赤色の  マークをカレンダー上に表示します。  のマークをクリックすると、解析結果の内容を表示することができます。
③ 最新の解析結果	最新の解析結果を表示します。危険なサイトだと判断された場合には赤く表示され、解析結果には危険の内容が表示されます。

解析結果カレンダーの  をクリックすると、解析結果の内容が表示されます。



① [http://\[redacted\]/index.html](http://[redacted]/index.html)

② 

③ **脅威名:Iframe Generic (GJS159)**
 貴社のWebサイトに不正に改ざんされたWebサイトのコンテンツが発見されました。不正に改ざんされたWebサイトとは、ウェブサイトの脆弱性を利用して不正に貴社のWebページに悪質なHTMLコードを追加したことを意味します。検知されたURLの内容に不正に追加されたHTMLコードがあるかを確認してください。「詳細を見る」をクリックすると悪質と思われるHTMLコードが表示されます。このHTMLコードが貴社のコンテンツでない場合は、Webサイトが改ざんされた可能性がありますので、このWebページの内容の確認をしてください。また、Webサーバに最新のパッチが適用されていることもご確認ください。万が一、貴社のコンテンツが誤検知されている場合は、お手数ですがサポートセンタへご連絡してください。

④ [詳細を見る](#)

⑤ [検知箇所を見る](#)

⑥ **検知した経路**
 ● [http://\[redacted\]/index.html](http://[redacted]/index.html)
 ▲ [http://\[redacted\]](http://[redacted])

解析結果の表示内容

項目名	内容
① URL 表示	危険と判断された URL が表示されます。
② 判定画面	危険と判断されたサイトの画像が表示されます。
③ 解析結果	どのような危険のあるサイトなのか表示します。
④ 解析結果の詳細	問題のあるソースコードがハイライト表示されます。
⑤ 検知した箇所を見る	検知箇所が可視化されます。
⑥ 検知した経路	検知した箇所の経路が表示されます。 「脅威名」の名称が表示されている場合には、検知経路が表示されます。

また、詳細レポートの「詳細を見る」をクリックすると、改ざんを検知したページのソースコードが表示され、問題のある箇所をハイライト表示します。

問題が見つかりました

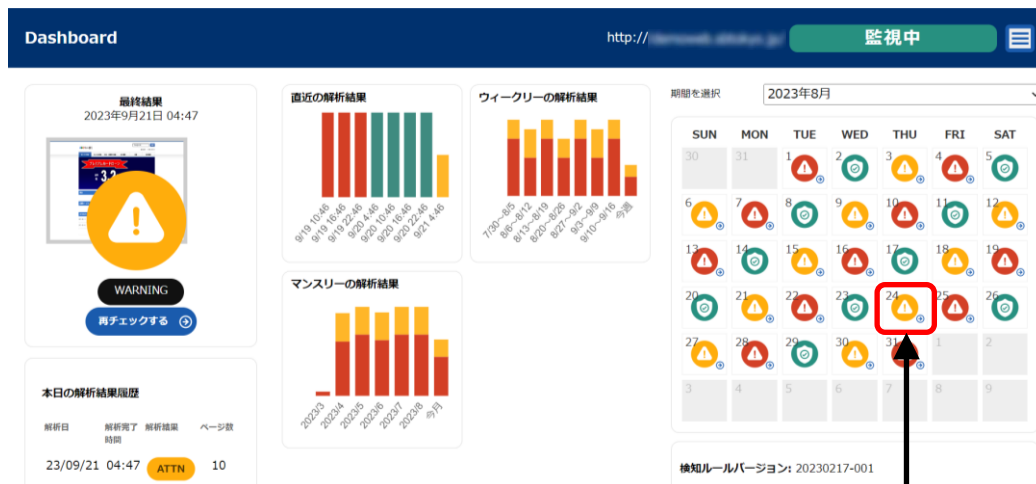
```
http://[redacted] /

以下のソースコード内のハイライト部に問題があります。

1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml2
2  <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
3  <head>
4  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5  <meta http-equiv="Content-Style-Type" content="text/css" />
6  <meta http-equiv="Content-Script-Type" content="text/javascript" />
7  <meta http-equiv="imagetoolbar" content="no" />
8  <meta name="description" content="" />
9  <meta name="keywords" content="" />
10 <link rel="stylesheet" href="css/common.css" type="text/css" />
11 <script type="text/javascript" src="js/jquery.js"></script>
12 <script type="text/javascript" src="js/common.js"></script>
13 <title>ABCネット銀行</title>
14 </head>
15 <body>
16 <div id="top">
17   <div id="header">
18     <h1><a href="index.html"></a></h1>
19     <div id="serch">
20       <form action="http://www.google.com/cse" id="cse-search-box">
21         <input type="hidden" name="cx" value="" />
22         <input type="hidden" name="ie" value="UTF-8" />
23         <dl>
24           <dt><input type="text" name="q" size="21" /></dt>
25           <dd><input type="image" src="images/serch.gif" alt="検索" name="sa" value="検索" />
26         </dl>
27       </form>
```

3.5 解析結果表示 黄色 (Warning・警告) クロスドメインスクリプト検知

許可設定をしていないクロスドメインスクリプトを検知すると、管理コンソールホームのマークが黄色の「Warning」(警告)に変化します。



黄色のマークをクリックすると
詳細ページが表示されます。

■ 詳細ページ

注意が必要です

2022年5月4日 10:03

① [https://\[redacted\].js](https://[redacted].js)

② **脅威名:[CrossDomain]**

ウェブページに、未確認のクロスドメインスクリプトを発見しました。クロスドメインスクリプトとは、自社サイト以外のドメインにあるスクリプトを実行させるようなコードが自社のサイトに記述されているという事です。スクリプト自体を確認し、正常なものである場合には「[クロスドメインの許可設定](#)」メニューにて許可してください。このスクリプトを記載した覚えがない場合にはウェブサイトの改ざんが発生している恐れがあります。その場合にはただちに該当HTMLを確認して、修正を行ってください。また許可設定を行うと、今後「警告」のメッセージ等が表示されなくなります。必要な場合には「[クロスドメインの許可設定](#)」メニューにて許可設定を削除すると、以降、再び警告を発するようになります。クロスドメインスクリプトの許可機能のON/OFFは「[クロスドメインの許可設定](#)」から行えます。

検知した経路

- [https://\[redacted\]kk.js](https://[redacted]kk.js)
- ↑ [https://\[redacted\]kaiso/](https://[redacted]kaiso/) ← ③
- ↑ [https://\[redacted\]cross/](https://[redacted]cross/)

解析結果の表示内容

	項目名	内容
①	URL 表示	クロスドメインを検知した URL が表示されます。
②	解析結果	クロスドメインの許可設定の説明
③	クロスドメインの経路	クロスドメインが見つかった経路を表示します。

「クロスドメインの許可設定」から自社のドメイン以外に利用しているスクリプトのドメインを設定しておくことによって、解析結果の「Warning」表示を「SAFE」に変更します。（設定の方法は、「5.7 クロスドメインの許可設定」をご覧ください。）

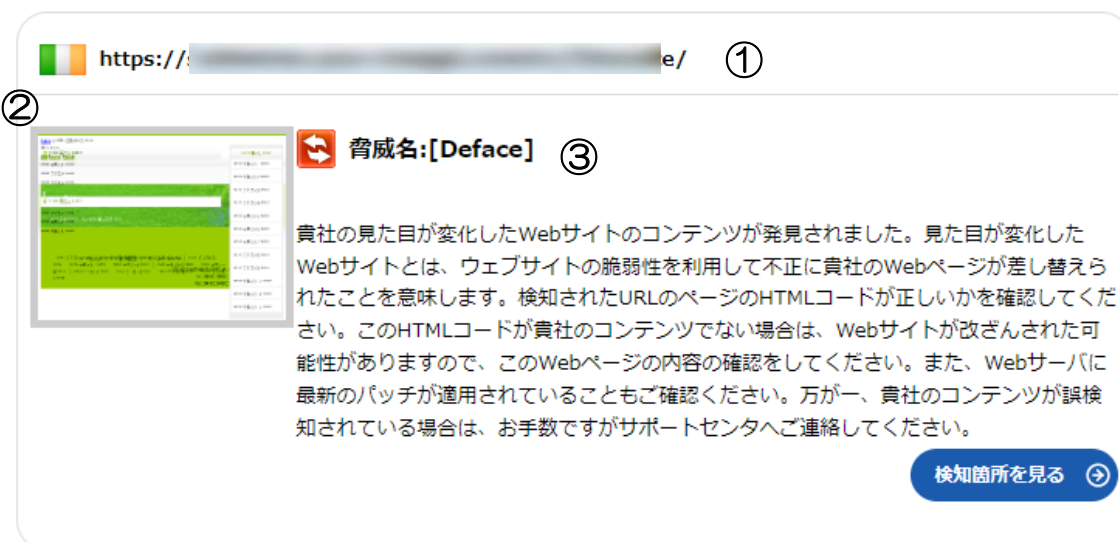
3.6 解析結果表示 黄色（Warning・警告）TOP ページの見た目変化検知

Top ページのコンテンツが著しく変化した場合に、検知メールが送信され詳細を管理コンソールで確認することができます。

※検知メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

注意が必要です

2022年5月14日 14:36



	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	判定画面	危険と判断されたサイトの画像が表示されます。
③	解析結果	どのような危険のあるサイトなのか表示します。

3.7 解析結果表示 黄色（Warning・警告）タグ・JavaScript の変化検知

JavaScript の変化を見ることにより改ざんを検知する「スクリプト変化検知エンジン」と HTML内の特定タグの src 属性や href 属性変化を検知する「リンクタグ変化検知エンジン」を実装しました。「タグ/JavaScript 変化検知」という項目で表示されます。詳細は管理コンソールで確認することができます。

注意が必要です

2022年5月16日 10:47

The screenshot shows a browser address bar with the URL `https://.../index.html` (labeled ①). Below it, a warning box titled 'タグ/JavaScript変化検知' (Tag/JavaScript Change Detection) is displayed. The warning message states: '前回の解析と比較して、タグ/JavaScriptに変化を検知しました。' (Compared to the previous analysis, a change in tags/JavaScript was detected). The '概要:' (Summary) section indicates '新しいスクリプトが追加されました' (A new script was added) (labeled ②). The '詳細:' (Details) section shows the start of a script tag: `<script type="text/javascript">` (labeled ③), followed by a blurred area representing the source code, and ending with `</script>`. A blue button labeled '検知箇所を見る' (View detection location) is located at the bottom right of the warning box.

	項目名	内容
①	URL 表示	タグ/JavaScript の変化を検知した URL が表示されます。
②	概要	タグ/JavaScript の変化の概要
③	変化したタグ/JavaScript	変化したソースコードを表示します。

3.8 解析結果表示 黄色（Warning・警告）EXE 解析検知

監視対象ページにある実行ファイルが、マルウェアと類似した動きをしている場合に警告を行う「表層解析エンジン」を実装しました。検知メールが送信され詳細を管理コンソールで確認することができます。

※検知メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

注意が必要です

2022年5月16日 11:27

① → https://: .exe

不正な挙動が疑われるファイルです。下記の挙動の詳細をご確認下さい。ファイルを確認いただき、正常なものである事が確認できた場合には「[除外設定のホワイトリスト](#)」メニューに該当URLを追加してください。HTMLに該当URLを記載した覚えがない場合や配置したファイルの中身が変更されている場合にはウェブサイトの改ざんが発生している恐れがあります。その場合、ただちに該当HTMLを修正いただくか、ファイルの入替えを行ってください。また、ホワイトリストに追加すると今後「警告」のメッセージ等が表示されなくなります。必要な場合には「[除外設定のホワイトリスト](#)」メニューにて該当URLを削除すると、再び警告を発するようになります。

② →

挙動の詳細

- アンチデバッグ機能(仮想環境での解析を不可にする)実装の可能性あり
- 暗号化の可能性あり

③ →

検知箇所を見る

	項目名	内容
①	URL 表示	危険と判断された URL が表示されます。
②	概要	ファイルの概要
③	解析結果	挙動の詳細を表示します。

3.9 改ざん検知時のメール送信

危険なサイトを検知すると、管理コンソールのアイコンが赤または黄色に変わると同時に登録いただいたメールアドレスに解析結果が送信されます。

メール本文には、検知したページの URL と内容が表示されます。

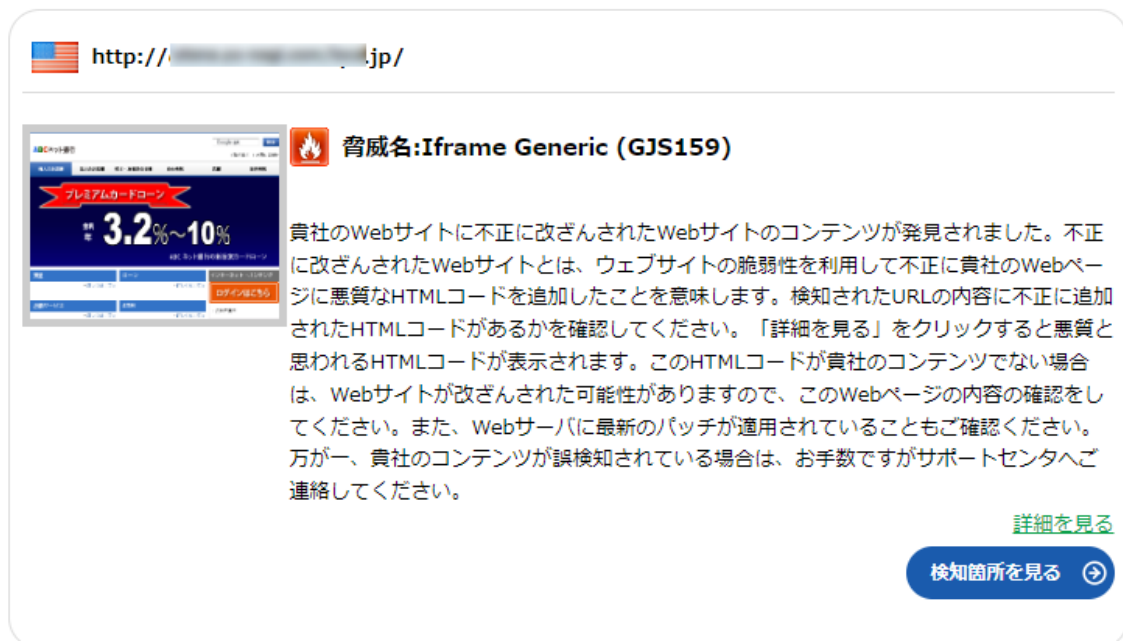
メール本文のリンクをクリックすると詳細ページにジャンプします。改ざんされている可能性があるウェブページの参照には十分ご注意の上、確認してください。

※検知メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

■ 詳細ページ

問題が見つかりました

2022年5月13日 15:29



改ざん検知以外のアラートメールは以下 5 種です。詳細は巻末の「付録 アラートメールサンプル」をご参照ください。

なおアラートメールは、管理コンソールから「メールを送信する」、「送信しない」を選択することができます。

- ・ Top ページのヘルスチェック検知時
- ・ 見た目変化検知時
- ・ クロスドメインスクリプト検知時
- ・ EXE 解析検知時
- ・ タグ・JavaScript 変化検知時

3.10 お知らせ機能

GreD Web 改ざんチェックからのお知らせやメンテナンスなどの情報を確認することができます。

管理画面には最新のお知らせが一件表示されます。タイトルをクリックすると詳細画面へ遷移します。

「一覧を見る：」をクリックすると、過去のお知らせ一覧が確認できます。

■ 一覧ページ

お知らせ一覧

掲載日	カテゴリ	タイトル
2023年02月22日	重要なお知らせ	新画面切替に関するお知らせ
2022年12月28日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年09月30日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年09月09日	重要なお知らせ	システムメンテナンスのお知らせ
2022年08月08日	重要なお知らせ	新画面に関するお知らせ
2022年06月30日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年04月14日	重要なお知らせ	システムメンテナンスのお知らせ
2022年04月01日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ
2022年03月07日	重要なお知らせ	システムメンテナンスのお知らせ
2022年01月01日	重要なお知らせ	定期システムメンテナンス スケジュールのお知らせ

■ 詳細ページ

お知らせ

2023年02月22日

【重要なお知らせ】新画面切替に関するお知らせ

- GREd Web改ざんチェックCloudは、2023/3/1に新画面へ移行しより多くの情報を可視化しお客様へ提供致します。
- 2022/8/9より、新画面を暫定URLで並行稼働していましたが、2023/6/1に暫定URLは廃止致します。
- 新画面では新たに、検知結果の推移グラフやGUIへのログイン履歴の参照が可能となっております。
- 新画面の利用は、Edge, Firefox, Chromeご利用を推奨いたします。

戻る

お知らせはメールでも受け取ることができます。

設定方法は「5.2 ユーザー情報の確認・変更」を参照してください。

4. 解析履歴

解析履歴やレポートの確認方法をご説明します。


4.1 解析履歴

過去の解析を確認することができます。

The screenshot shows the '解析履歴' (Analysis History) page. The page title is '解析履歴' and the status is '監視中'. The left sidebar contains navigation items: 'ホーム', '解析履歴', 'レポート作成', and '解析内容の設定'. The main content area displays a table of analysis results. A warning message states: '解析履歴の表示期間は2カ月です。' (The display period for analysis history is 2 months). The table has the following data:

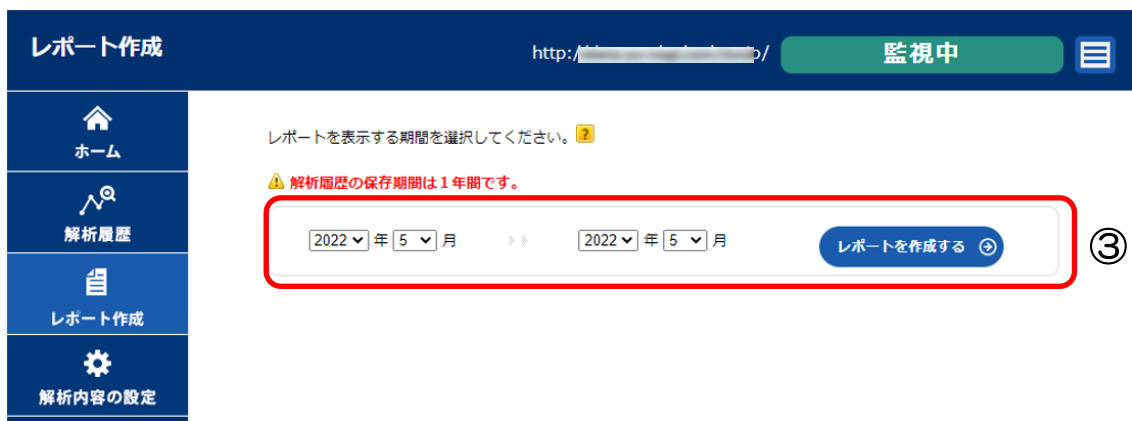
解析日	解析完了時間	解析結果	URL数
2022年05月16日	05:10	改ざんを発見しました	10
2022年05月15日	17:10	注意が必要です	10
2022年05月15日	05:10	注意が必要です	10
2022年05月14日	17:10	問題はありませんでした	10
2022年05月14日	05:10	問題はありませんでした	10
2022年05月13日	17:10	改ざんを発見しました	10
2022年05月13日	15:29	改ざんを発見しました	10


At the bottom of the page, there is a 'ダウンロード' (Download) button highlighted with a red box and a circled number 3. Below the button, it says: '※2カ月分の解析履歴をダウンロードします' (Download 2 months of analysis history).

- ① 管理画面左上の  をクリックし、「解析内容の設定」に遷移します。
- ② 左側の「解析履歴」をクリックします。
- ③ 解析日、解析完了時間、解析結果、ページ数を新しいものから順に表示します。赤、黄色の項目はクリックすると詳細ページにジャンプします。
「ダウンロード」をクリックする事で、CSV 形式のファイルでダウンロード可能です。

4.2 レポート作成

左側にある「レポート作成」をクリックします。
一定期間の解析結果の統計情報を見ることができます。



- ① 管理画面左上の  をクリックし、「解析内容の設定」に遷移します。
- ② 左側の「レポート作成」をクリックします。
- ③ 統計を出したい期間（1 か月単位）を指定し「レポートを作成する」ボタンをクリックすると、指定された期間の統計概要と月ごとの解析結果が表示されます。

GREDD Web改ざんチェック Cloud 2022年5月16日 13:48

GREDD Web改ざんチェック レポート

- 解析対象ドメイン: http:// /
- 解析期間: 2022年5月~2022年5月
- 解析結果: 問題あり

2022	5月
改ざんを通知した回数	6
貴社のウェブページ数(平均)	10

改ざん内容の詳細

- [検知日]2022年5月13日 15:29
- [検知ページ]http:// /index.html

警告 貴社のWebサイトに不正に改ざんされたWebサイトのコンテンツが発見されました。不正に改ざんされたWebサイトとは、ウェブサイトの脆弱性を利用して不正に貴社のWebページに悪質なHTMLコードを追加したことを意味します。検知されたURLの内容に不正に追加されたHTMLコードがあるかを確認してください。このHTMLコードが貴社のコンテンツでない場合は、Webサイトが改ざんされた可能性がありますので、このWebページの内容の確認をしてください。また、Webサーバに最新のパッチが運用されていることもご確認ください。万が一、貴社のコンテンツが誤検知されている場合は、お手数ですがサポートセンタへご連絡してください。

詳細

脅威名:Iframe Generic (GJS159)

レポートを印刷する

	項目名	内容
①	統計概要	解析したサイトと期間、解析結果
②	統計詳細	月別の統計結果
③	印刷	レポートを印刷します。

4.3 週間レポートメール

週に1度(月曜日)に、1週間の解析結果をメールでお知らせします。

※メールの詳細については、巻末の「付録 アラートメールサンプル」をご参照ください。

5. 各種設定

各種機能の追加・変更等の設定方法をご説明します。

5.1 ユーザー管理

新しいユーザー（サブユーザー）を追加します。管理画面へアクセスが可能なユーザーを5名まで追加登録できます。申込時に登録したメインユーザーのみサブユーザーの登録が可能です。



サブユーザー

サブユーザーを追加します。 ?

サブユーザーご担当者名(お名前)	<input type="text"/>
ログインID	<input type="text"/>
アラート用メールアドレス	<input type="text"/> <small>※こちらのアドレスにサブユーザー登録完了の通知メールが届きます。</small>
アラートメール通知	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
使用言語	<input checked="" type="radio"/> 日本語 <input type="radio"/> 英語
タイムゾーン	GMT+09:00;JST;Asia/Tokyo
アクセスの権限	<input type="checkbox"/> 全て選択 <input type="checkbox"/> デモサイト

追加する

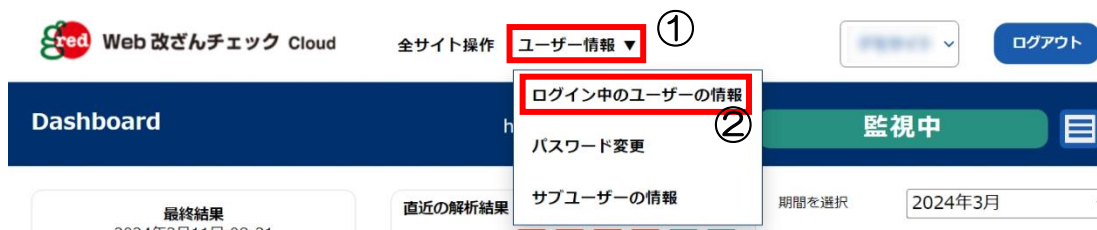
- ① ヘッダーの「ユーザー情報」をクリックします。
- ② 「サブユーザー」をクリックします。
- ③ サブユーザーご担当者名（お名前）、ログイン ID、アラート用メールアドレス、アラートメールの受け取りの有無、使用言語（日本語/英語）、タイムゾーン、アクセスの権限を入力し、「追加する」をクリックします。

※ログイン ID は一度設定しますと変更はできませんのでご注意ください。

5.2 ユーザー情報の確認・変更

アラート用メールアドレス、名前の変更が行えます。

また、週間レポートメール、アラートメールの受け取りの有無、使用言語（日本語/英語）、タイムゾーン、二要素認証もここで変更できます。



ユーザー情報

ユーザー情報を変更します。?

ユーザID(ログインID)	[ユーザーID]	
アラート用メールアドレス	[メールアドレス]	
ご担当者名(お名前)	[お名前]	
週間レポートメール通知	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
アラートメール通知 ?	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
	改ざん検知時	[有効の場合は送信します]
	Topページのヘルスチェック検知時	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
	見た目変化検知時	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
	クロスドメインスクリプト検知時	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
	マルウェア解析検知時	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
お知らせ通知 ※アラート用メールアドレスに通知されます。	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
	重要なお知らせ 機能追加・変更 サービス・システム仕様変更 メンテナンス など	[有効の場合は送信します]
	新サービス・オプションのご案内	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
使用言語	<input checked="" type="radio"/> 日本語 <input type="radio"/> 英語	
タイムゾーン	GMT+09:00;JST;Asia/Tokyo	
二要素認証 ?	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	

※ユーザID (ログインID) は変更できません。



ユーザID(ログインID)	XXXXXXXXXXXXXXXXXXXX
アラート用メールアドレス	XXXXXXXXXXXXXXXXXXXX@XXXXXXXXXXXX
ご担当者名(お名前)	XXXXXXXXXXXXXXXXXXXX
週間レポートメール通知	有効
アラートメール通知	有効 [メール送信のタイミング] -改ざん検知時 -Topページのヘルスチェック検知時 -見た目変化検知時 -クロスドメインスクリプト検知時 -マルウェア解析検知時 -タグ/JavaScript変化検知時
お知らせ通知	有効 [通知内容] -重要なお知らせ -新サービス・オプションのご案内
使用言語	日本語
タイムゾーン	Asia/Tokyo
二要素認証	有効

変更はまだ完了していません。

次の画面で表示されるQRコードまたは登録用コードを使用して認証アプリへ登録してください。



- ① ヘッダーの「ユーザー情報」をクリックします。
- ② 「ログイン中のユーザーの情報」をクリックします。
- ③ 設定変更などを行い、「確認する」をクリックします。
※「お知らせ通知」は申込時に登録したメインユーザーのみ設定できます。
- ④ 確認画面にて変更内容を確認し、「変更する」をクリックします。

二要素認証を無効から有効へ変更すると以下の画面を表示します。

ユーザー情報

ユーザー情報を変更しました。

QRコードまたは登録用コードを使用して認証アプリ(Google AuthenticatorまたはMicrosoft Authenticator)へ登録してください。

⚠ 認証アプリへ登録する前に別ページへ遷移したり画面を閉じたりしないでください。

認証アプリへ登録せずにログアウトした場合は、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。認証アプリの削除やデバイスの変更・紛失等によりログインできなくなった場合も、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。



登録用コードを表示する

認証アプリへ登録完了

こちらの画面で QR コードまたは登録用コードを使用して認証アプリ (Google Authenticator または Microsoft Authenticator) へ登録してください。次回以降のログイン時には、ID とパスワードに加えて認証アプリで取得するワンタイムパスワードを使用してログインしてください。

認証アプリへ登録せずにログアウトした場合は、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。認証アプリの削除やデバイスの変更・紛失等によりログインできなくなった場合も、ログイン画面からパスワードを再設定して二要素認証を無効にしてください。

5.3 パスワードの変更

ログインパスワードの変更は、ここから行ってください。

Web 改ざんチェック Cloud 全サイト操作 **ユーザー情報** ① ログアウト

Dashboard 監視中

最終結果 2024年3月11日 00:24 直近の解析結果 サブユーザーの情報 期間を選択 2024年3月

Web 改ざんチェック Cloud 全サイト操作 ユーザー情報 ログアウト

パスワード

現在のパスワード

新しいパスワード 使用可能な文字は半角英数字と記号 (!.?+\$%#&*=@)で、10文字以上50文字以下。
全角文字、ログインIDと同じものは使えません。
英文字と数字をそれぞれ1文字以上入れてください。

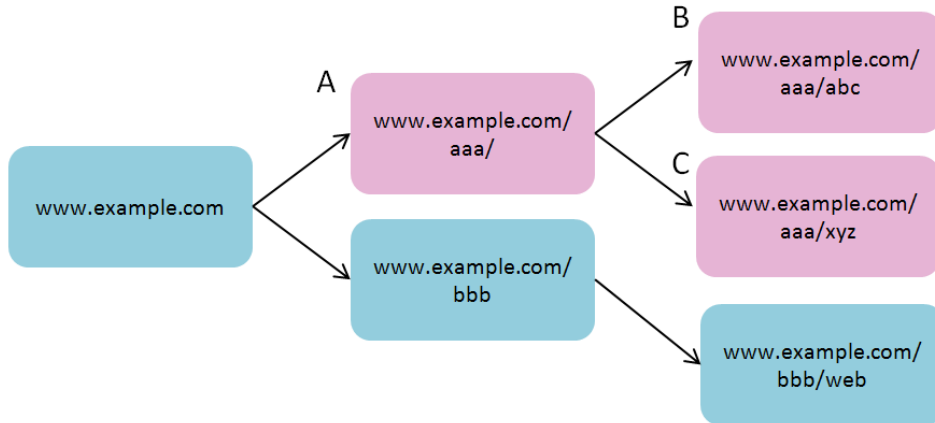
新しいパスワード (確認用)

戻る **変更する** ③

- ① ヘッダーの「ユーザー情報」をクリックします。
- ② 「パスワード変更」をクリックします。
- ③ 現在のパスワードと新しいパスワードを入力し、「変更する」をクリックします。

5.4 除外 URL の登録

除外 URL の設定は、パス（ディレクトリ）指定を最大 100 個まで行うことができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。



※A(www.example.com/aaa/)を指定した場合、BとCも解析対象から除外されます。



除外URLは、パス（ディレクトリ）指定を最大100個まで設定することができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。?

除外URLに登録したいパス (ディレクトリ) ③

正規表現 ? 使用する

登録する ➔

除外URLリスト

登録されている除外URLはありません

- ① 管理画面左上の をクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「除外設定」内の「除外URL」をクリックします。
- ③ 「除外URLに登録したいパス（ディレクトリ）」欄に任意のURLもしくは正規表現を入力し「登録する」をクリックします。

※除外したい URL については、正規表現を使用することも可能です。正規表現を使用したい場合は、「正規表現」にチェックを入れて登録してください。

■ 記述例

設定	効果
www.foo.bar	www.foo.bar で終わるドメインの URL をクロールしない。 例) 次の URL はクロールしません http://www.foo.bar/top.html http://www.foo.bar/map.html http://ex1.www.foo.bar/
foo.bar	foo.bar で終わるドメインの URL をクロールしない。 例) 次の URL はクロールしません http://foo.bar/top.html http://www.foo.bar/ http://blog.foo.bar/user1/entry.html
www.foo.bar/blog	www.foo.bar で終わるドメインの/blog で始まるパスの URL をクロールしない。 例) 次の URL はクロールしません http://www.foo.bar/blog/ http://www.foo.bar/blog/entry/1.html

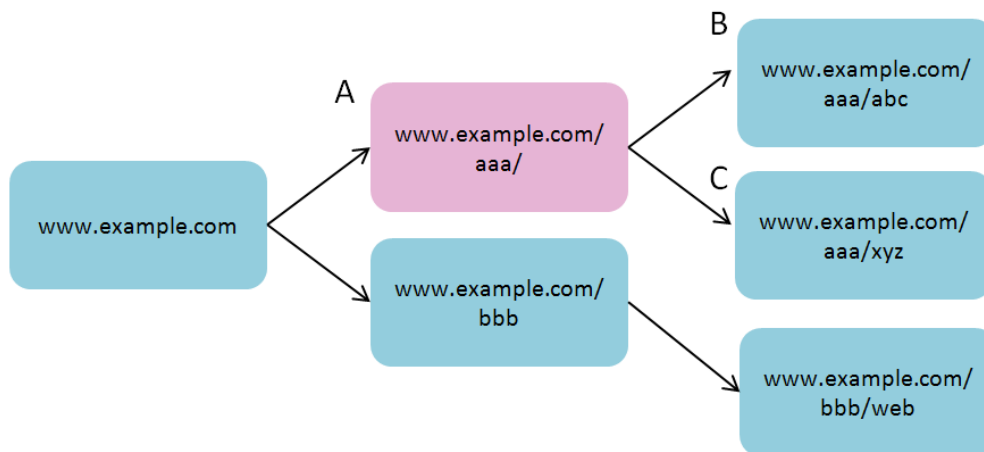
■ 正規表現を使用する場合の記述例

設定	効果
www¥.foo¥.bar/.*blog/	ドメインが www.foo.bar で終わり、2 つ目以降のディレクトリが blog である URL を除外する。 例) 次の URL はクロールしません https://www.foo.bar/aaa/blog/index.html https://www.foo.bar/bbb/blog/index.html 注意点 *(アスタリスク)はワイルドカードではなく正規表現になる為、上記のように任意のディレクトリを除外する際は*のみの指定では除外出来ません。 .(ドット)は正規表現では任意の 1 文字として扱われますので、正規表現として扱わない場合は、¥(エスケープ)を付加してください。


5.5 ホワイトリストの登録

ホワイトリストは、あらかじめ問題が無い事がわかっている URL を指定して、常に「OK」という判断を行うリストです。最大 10 個まで指定することが可能です。

このリストに指定した URL は解析ページ数としてカウントされますが必ず「OK」という結果になります。ページにリンクがあった場合にはそのリンクから先もクローリングします。ただし、このリストに指定したページのみ「OK」となる事に注意してください。




※A(www.example.com/aaa/)を指定した場合、このページは必ず「OK」という解析結果となります。 B と C は通常通り解析が行われます。

- ① 管理画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「除外設定」内の「ホワイトリスト」をクリックします。
- ③ 「ホワイトリストに登録したい URL」欄に任意の URL を入力し「登録する」をクリックします。

5.6 監視の ON/OFF とウェブ解析対象階層の指定

GREED Web 改ざんチェック Cloud 自体の監視の ON/OFF を管理コンソールで行うことができます。また、解析対象の階層数を指定する事により、解析ページ数の調整が可能です。指定された階層以降はページが存在していても解析を行わず、解析対象ページ数としてもカウントいたしません。


監視の ON/OFF の設定

- ① 画面左上の  をクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「基本設定」内の「監視の ON/OFF と基本設定」をクリックします。
- ③ 有効または、無効にチェックを入れて「変更する」ボタンをクリックします。
- ④ 「ウェブ解析対象階層の指定」欄に解析対象の階層数を入力し「変更する」をクリックします。
- ⑤ 検知するレベル「スクリプトタグに変化がある場合に検知」、「特定のタグに変化がある場合に検知 (スクリプトタグ含む)」、「無効」のいずれかを選択し「変更する」ボタンをクリックします。

※デフォルトでは「スクリプトタグに変化がある場合に検知」がオンになっています。

5.7 クロスドメインの許可設定

ウェブ改ざんチェックの「クロスドメインスクリプト管理・警告機能」は、自社サイト外に誘導するスクリプトがウェブページに埋め込まれた場合に「警告」を行います。あらかじめ任意で埋め込んだ外部に飛ばすスクリプトは、許可リストに登録してください。

- ① 画面左上の  をクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「クロスドメイン設定」内の「クロスドメイン検知」をクリックします。
- ③ クロスドメインスクリプトの「有効/無効」の設定ができます。いずれかにチェックを入れます。
- ④ 「許可リスト:クイック登録」では見つかったクロスドメインスクリプトが表示されます。許可する場合は、ボックスにチェックを入れて「登録する」ボタンをクリックしてください。
- ⑤ 「許可リスト:編集」では登録している項目を削除することもできます。削除したい URL のチェックボックスにチェックを入れ、「削除する」ボタンをクリックします。

・クロスドメイン共通許可リスト

全サイトに共通しているクロスドメインを許可リストに登録することができます。

自社ドメイン以外のスクリプト(クロスドメインスクリプト)が発見された場合に警告を行います。ここでは、安全なクロスドメインスクリプトに対して警告しないように、自社のドメイン以外に利用しているスクリプトのドメインを許可リストに設定しておくことができます。
(全サイトに共通して許可するドメインを設定する場合は [こちら](#) ^①を設定することができます。)

クロスドメインスクリプトの検知機能 有効 無効

適用する 

クロスドメイン共通許可リスト

ここでは、安全なクロスドメインスクリプトに対して警告しないように、自社のドメイン以外に利用しているスクリプトのドメインを全サイト共通の許可リストに設定しておくことができます。

共通許可リスト：追加

許可リストにクロスドメインスクリプト使用中のドメイン名、もしくはホスト名が登録できます。

許可リストに登録したい
クロスドメイン **登録する**  ②

共通許可リスト：編集

現在登録しているクロスドメインスクリプト一覧です。登録している項目を削除する事もできます。

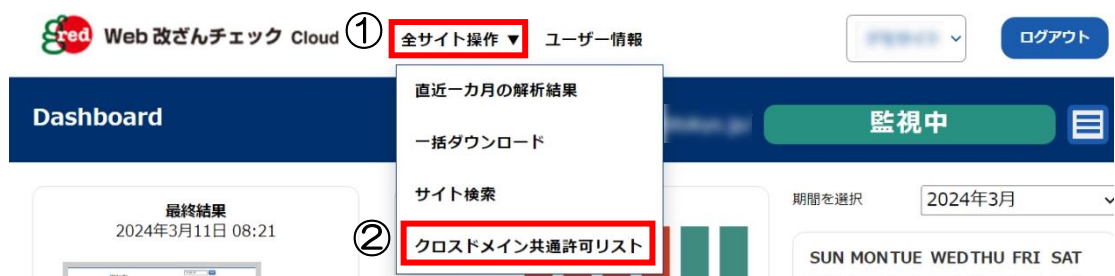
すべてチェック

securebrain.co.jp

削除する  ③

- ① 「こちら」をクリックします。
- ② 「共通許可リスト：追加」に URL・ドメインを入力し「登録する」ボタンをクリックします。
- ③ 「共通許可リスト：編集」では登録している項目を削除することができます。削除したい URL・ドメインにチェックを入れ「削除する」ボタンをクリックします。


クロスドメイン共通許可リストの設定画面はヘッダーからもアクセスが可能です。



- ① ヘッダーの「全サイト操作」をクリックします。
- ② 「クロスドメイン共通許可リスト」をクリックします。
- ③ クロスドメイン共通許可リストの設定画面に遷移します。

5.8 改ざん検知時のページ切り替え機能の設定

改ざんが確認された場合に、自動でページを切り替える機能が利用できます。

- ① 管理画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「オプション」内の「改ざん時切り替え機能」をクリックします。
- ③ お客様専用のタグが生成されます。<html>タグのすぐ後に取得したタグを挿入して下さい。

■ タグのサンプル ※切り替え機能のタグはお客様ごとに異なります。

```
<script type="text/javascript" src="https://www3.gred.jp/saas/gred_checker.js?sid=■■■■">
</script>
```

お客様独自のメンテナンスページを表示させる場合には末尾に【&redirect_url=" 挿入したいメンテナンスページの URL "】を追加してください。

・切り替え機能設定


ページ切り替え機能の有効/無効を設定します。

切り替え機能設定 有効 無効

設定する 

「有効」を選択すると切り替えに関するオプションが表示されます。

切り替え機能設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
切り替え機能適応範囲	<input type="radio"/> 検知ページのみ <input checked="" type="radio"/> 全ページ 上記のタグを挿入した解析対象ドメインのページのうち検知ページまたは全ページを切り替えます。
クロスドメインがあった場合	<input type="radio"/> 切り替える <input checked="" type="radio"/> 切り替えない

[設定する](#) 

・ 切り替え画面サンプル

【メンテナンス画面】




※ウェブ改ざんチェックのサービスを終了した場合は、埋め込んだタグの削除をお願いします。

5.9 GREd 証明書の設定

サイトが改ざんされていないことを証明できる「GREd 証明書」が利用できます。この証明書をサイトに表示し、クリックすると検証結果が表示されます。

The screenshot shows the '解析内容の設定' (Analysis Content Settings) page. The top navigation bar includes a home icon, a URL field, and a '監視中' (Monitoring) status. The left sidebar contains navigation items: 'ホーム' (Home), '解析履歴' (Analysis History), 'レポート作成' (Report Creation), '解析内容の設定' (Analysis Content Settings), and '簡易脆弱性診断' (Simple Vulnerability Diagnosis). The main content area is divided into three columns: '基本設定' (Basic Settings), '除外設定' (Exclusion Settings), and 'クロスドメイン設定' (Cross-Domain Settings). Below these is an 'オプション' (Options) section where the 'GREd証明書' (GREd Certificate) item is highlighted with a red box and a circled '2'. A note at the bottom states: '[ウェブ解析開始URL・ウェブ解析対象ドメインを変更されたい際には販売元までお問い合わせください]'.

- ① 管理画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 画面中央のメニューから「オプション」内の「GREd 証明書」をクリックします。
- ③ お客様専用のタグが生成されます。そのタグをページ内の GREd 証明書を表示させたい部分に挿入して下さい。

■ タグのサンプル※GREd 証明書のタグはお客様ごとに異なります。

```
<a href="https://www2.gred.jp/saas/ratingVerify.htm?sid=4^10"
onclick="window.open('https://www2.gred.jp/saas/ratingVerify.htm?sid=4^10',
'_blank', 'width=600,height=600,resizable=no,menubar=yes,toolbar=yes');
return false;" oncontextmenu="alert('この画像はコピーできません。');return
false;"><img height="40" border="0" width="85" src="https://www2.gred.jp
/saas/seal.gif?sid=4^10" onerror = "javascript:src = 'https://www.gred.jp
```

[gred証明書の検証ページを見る](#)





表示内容

Web サイト名:

最終解析完了時間:

(最後にチェックした時間が表示されます)

解析結果:

(最後に解析を行った結果が表示されます)


※GREd Web 改ざんチェック Cloud のサービスを終了した場合は、埋め込んだタグの削除をお願いします。

5.10 非リンク URL の登録

TOP の URL から辿れない URL を管理画面から非リンク URL として登録することで解析対象にすることができます。登録できる非リンク URL は、解析対象ドメインのみとなります。自動的にリンクを辿らないため、解析対象とする URL を 1 件ずつ登録する必要があります。最大 20 件まで登録出来ます。ご契約されている URL 数の範囲内で TOP からリンクされている URL と、このページで登録した非リンク URL を解析します。TOP からリンクされている URL の解析終了後に非リンク URL を解析します。解析中に契約されている URL 数を超えた場合は、その時点で解析を終了します。

なお、本設定で登録した URL は、「6.6 リンク切れ検知機能」「6.7 リンク構造可視化機能」の対象外となります。

非リンク URL 登録画面表示方法

- ① 管理画面左上の  をクリックし、「解析内容の設定」に遷移します
- ② 「オプション」メニューから「非リンク URL の登録」をクリックします。
- ③ 非リンク URL の登録画面が表示されます。

非リンクURLの登録 https://[redacted].jp/ 監視中 ☰

ホーム
解析履歴
レポート作成
解析内容の設定
簡易脆弱性診断

リンクしていないURLを解析出来るように登録します。1つずつ、もしくはファイルをアップロードすることでURLを登録出来ます。登録出来る件数は最大20件までです。(重複するURLや解析対象ではないドメインのURLは登録出来ません。) ?

1つずつ入力

URL

登録 ⌵

ファイルからアップロード

ファイルを選択 選択されていません

ファイルをアップロード ⌵

※ファイルフォーマットは改行区切りです。

登録済みのURLリスト

全 2件

URL	アクション
http://www.test.co.jp/test1.html	削除
http://www.test.co.jp/test2.html	削除

リストのクリア ⌵

非リンク URL の登録方法(二通り)

① URL を一つずつ登録する

URL 入力ボックスに URL を入力し「登録」ボタンをクリックしてください。下部の登録済みの URL リストに追加されます。

② ファイルからアップロードする

「ファイルを選択」ボタンから改行区切りの URL リストを選択し「ファイルをアップロード」ボタンをクリックしてください。下部の登録済みの URL リストに追加されます。

非リンク URL の削除方法(二通り)

① 削除ボタンから一つずつ削除する

登録済み URL リストのアクション項目にある削除ボタンをクリックします。該当の URL がリストから削除されます。

② 一括削除する

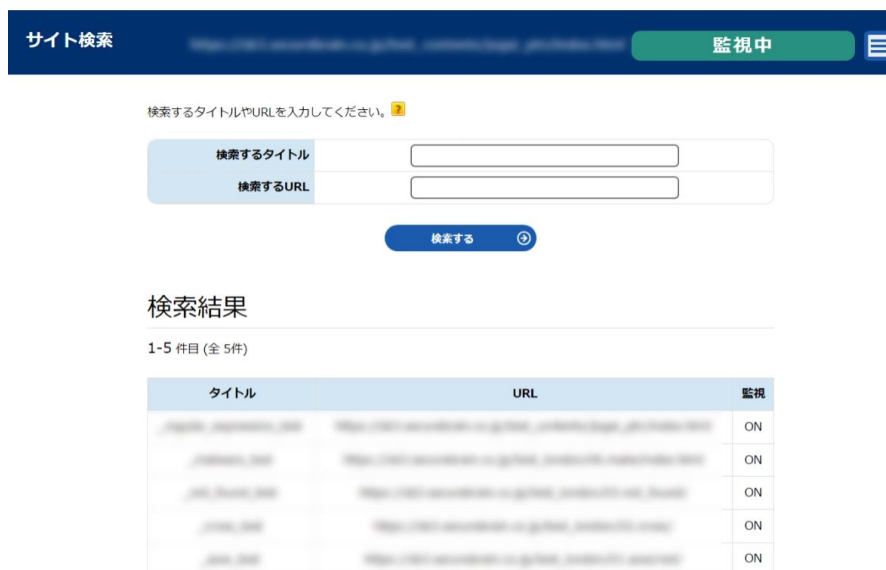
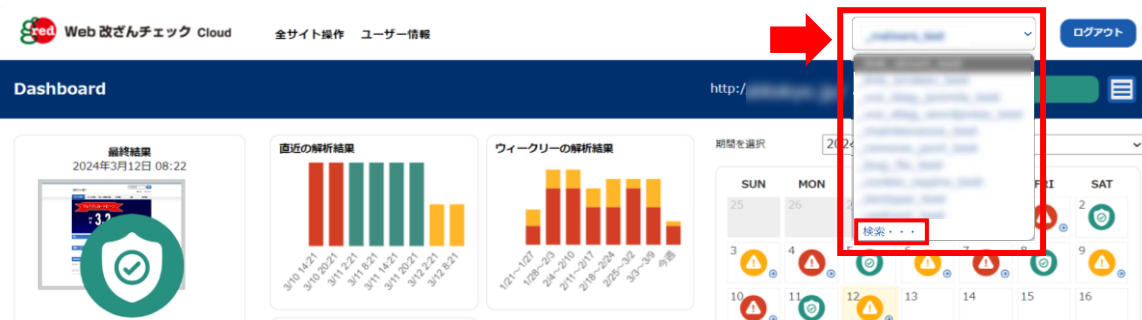
登録済み URL リストの下部にある「リストのクリア」ボタンをクリックします。リストからすべての URL が削除されます。

6. その他の機能・サービス

各種設定、サービスの提供は、管理コンソールより行います。

6.1 解析サイトの検索

複数の解析サイトを1つの管理コンソールで管理している場合、確認したい解析サイトの検索ができます。解析サイトが10以上ある場合に「検索・・・」リンクが表示され、クリックすると該当する解析サイトの管理コンソールへのリンク一覧が表示されます。



ヘッダーの「全サイト操作」をクリックし「サイト検索」からアクセスも可能です。



6.2 オンデマンドチェック機能

改ざんを検知し、修復を行った際に、問題がないか確認できるよう、即時チェックを行う機能です。1日に2回まで使用可能です。



6.3 GREd 証明書

この証明書をお客様のサイトに表示すれば、GREd によって守られている検証結果を表示させることができます。HTML の `img` タグにより GREd 証明書のイメージを埋めこみます。タグをページ内の GREd 証明書を表示させたい部分に挿入して下さい。エンドユーザーが GREd 証明書をクリックすると、ポップアップ画面が表示され、そのページについて GREd での解析結果が表示されます。

GREd 証明書のタグの入手方法は「GREd 証明書の設定」をご覧ください。



クリックすると
以下の画面が開
きます。



6.4 ポートスキャン診断機能

ポートスキャン診断は、ポートスキャン診断を選択し診断実行ボタンをクリックするだけで、対象のポートが開いているか閉じているかを調査します。開いているポートに脆弱性情報が提供されている製品がある場合は、情報を提供しているウェブサイトの URL 等、参照情報を表示します。

ポートスキャン診断は以下のポートに対して診断を実施します。

診断ポート：20-22、53、80、443、445、1433、3306、8080、8887、10001、20001、30001、40001、50001、60001

【使用方法】

簡易脆弱性診断 https:// [redacted] 監視中 ☰ ①

診断メニュー ポートスキャン診断結果 Joomla診断結果

診断する項目を以下から選択してください。

ポートスキャン診断 ③
ポートスキャンでは以下のポートに対して診断を実施します。
 診断ポート:20-22,53,80,443,445,1433,3306,8080,8887,10001,20001,30001,40001,50001,60001

Joomla診断 ②

[免責事項]利用者は自らの責任及び判断において本サービスを利用するものとし、診断結果、および直接的・間接的を問わず利用者が本サービスを利用したことにより生じたあらゆる損害、損失、責任、負担に対して 当社は一切責任を負わないものとします。

④ 診断実行 診断実行の限度数は項目数に関わらず月に5回です ?
 診断残回数:5回
(診断を実行する場合は一度だけクリックしてください)

⑤

最終診断日時：2022/05/11 14:12:32 結果更新


[-] ホスト情報
 ステータス：up
 スキャンしたポート：20-
 22,53,80,443,445,1433,3306,8080,8887,10001,20001,30001,40001,50001,60001
 開いているポート数：2
 閉じているポート数：0
 フィルタされているポート数：15
 その他のポート数：0
 ホスト名：[REDACTED]

[-] OS情報
 名前：
 精度：0%

[-] アドレス
 IPv4：46.51.245.61
 IPv6：
 MACアドレス：

[-] ポート情報

ステータス	ポート番号	プロトコル	サービス	プロダクト名とバージョン
filtered	20	tcp	ftp-data	
filtered	21	tcp	ftp	
filtered	22	tcp	ssh	
filtered	53	tcp	domain	
🚩 open	80	tcp	http	Apache httpd 2.2.34 +脆弱性対策情報
🚩 open	443	tcp	http	Apache httpd 2.2.34 +脆弱性対策情報

- ① 管理画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 左側の「簡易脆弱性診断」をクリックします。
- ③ 「ポートスキャン診断」にチェックを入れます。
- ④ 「診断実行」をクリックします。
- ⑤ 診断完了後、ポートスキャン診断結果のタブに結果が表示されます。

【ご注意事項】

※1) 本診断の特性上、不正アクセス検知システム（サーバ監視ツールや、IPS/Firewall など）に不正なアクセスとして検知される可能性がございます。診断を行う際は、事前に関連部署に対して脆弱性診断実施の了承、並びに本脆弱性診断サービスからのアクセスを一時的に監視対象から外していただく等のご対応をお願いいたします。「診断実行」ボタンをクリックすると上記注意事項が書かれたポップアップが表示され、注意書きに同意をいただいた上でスキャンを開始する仕様になっています。本ツールの IP アドレスを確認したい場合はお問い合わせください。

※2) 診断実行の限度数は、診断メニューにかかわらず月初～月末に 5 回です。各診断を 1 つのみを実行した場合も 1 回カウントされます。各診断を同時に行った場合は

1 回のカウントになります。

※3) 本サービスを使用した場合、以下の免責事項に同意したものとします。本免責事項は診断実行ページに記載しています。

【免責事項】

利用者は自らの責任及び判断において本サービスを利用するものとし、直接的・間接的を問わず 利用者が本サービスを利用したことにより生じたあらゆる損害、損失、責任、負担に対して 当社は一切責任を負わないものとします。

6.5 Joomla 簡易脆弱性診断機能


Web サイトを Joomla で構築されているお客様は、GREd の管理コンソール内からワンクリックで、現在使用している Joomla のバージョン情報やご利用のコンポーネント情報を検出し、検出されたバージョンおよびコンポーネントに脆弱性がないかをチェックすることができます。脆弱性ありと診断した場合、脆弱性のあるバージョンと脆弱性の内容を表示し、アップデートなどの情報を提供しているウェブサイトの URL 等、参照情報を表示します。

【使用方法】

The screenshot displays the Joomla vulnerability diagnosis interface. At the top, there is a header with the title '簡易脆弱性診断' and a '監視中' (Monitoring) status. Below the header, there are navigation tabs for '診断メニュー', 'ポートスキャン診断結果', and 'Joomla診断結果'. The main content area is titled '診断メニュー' and contains a list of diagnosis options. The 'Joomla診断' option is selected and highlighted with a red box and callout 3. Below the options, there is a '診断実行' button highlighted with a red box and callout 4. The sidebar on the left contains various navigation options, with '簡易脆弱性診断' highlighted by a red box and callout 2. A red box and callout 1 highlight the hamburger menu icon in the top right corner.

The screenshot shows the Joomla diagnosis results page. The page title is "Joomla診断結果". The left sidebar contains navigation options: Home, Analysis History, Report Creation, Analysis Content Settings, and Simple Vulnerability Diagnosis. The main content area shows the following information:

- 最終診断日時: 2021/12/22 17:18:21 結果更新
- [Joomla使用バージョン]
Joomla 3.6.0
- [Joomla基本脆弱性情報]
- 脆弱性名: Joomla! 3.4.4 < 3.6.4 - Account Creation / Privilege Escalation
CVE:
CVE-2016-8870
CVE-2016-8869
参照情報:
<https://www.exploit-db.com/exploits/40637/>
- 脆弱性名: Joomla! Core Remote Privilege Escalation Vulnerability
CVE:
CVE-2016-9838
参照情報:
<https://www.exploit-db.com/exploits/41157/>
- 脆弱性名: Joomla! Core Security Bypass Vulnerability
CVE:

- ① 管理画面左上のをクリックし、「解析内容の設定」に遷移します。
- ② 左側の「簡易脆弱性診断」をクリックします。
- ③ 「Joomla 診断」にチェックを入れます。
- ④ 「診断実行」をクリックします。
- ⑤ 診断完了後、Joomla 診断結果のタブに結果が表示されます。

【ご注意事項】

※1) 本診断の特性上、不正アクセス検知システム（サーバ監視ツールや、IPS/Firewall など）に不正なアクセス攻撃として検知される可能性がございます。診断を行う際は、事前に関連部署に対して脆弱性診断実施の了承、並びに本脆弱性診断サービスからのアクセスを一時的に監視対象から外していただく等のご対応をお願いいたします。
本ツールの IP アドレスを確認したい場合はお問い合わせください。

※2) 本脆弱性診断が可能な回数は、月初～月末に 5 回です。
各診断を 1 つのみを実行した場合も 1 回カウントされます。各診断を同時に行った場合は 1 回のカウントになります。

※3) 本サービスを使用した場合、以下の免責事項に同意したものとします。本免責事項は診断実行ページに記載しています。


【免責事項】

利用者は自らの責任及び判断において本サービスを利用するものとし、直接的・間接的を問わず利用者が本サービスを利用したことにより生じたあらゆる損害、責任、負担に対して当社は一切責任を負わないものとします。

6.6 リンク切れ検知機能

リンクが切れているページを検知しリスト表示します。リンク切れ検知の対象となるのは GREd のクローラが辿るリンクのみです。サーバから 404 エラー応答のあった URL をリンク切れとして検知します。表示されるのは最新の解析結果のみとなります。リンク切れを検知させるには、TOP 画面左メニューの「解析内容の設定」をクリックしオプションメニューの「リンク切れ検知設定」をクリックしてください。

The image shows three sequential screenshots of the GREd Web interface. The first screenshot shows the '解析内容の設定' (Analysis Content Settings) page with a red box around the menu icon (1). The second screenshot shows the 'オプション' (Options) menu with a red box around the 'リンク切れ検知設定' (Link Break Detection Settings) option (2). The third screenshot shows the 'リンク切れ検知設定' (Link Break Detection Settings) page with a red box around the '有効' (Effective) radio button and the '設定する' (Set) button (3).

- ① 管理画面左上の  をクリックし、「解析内容の設定」に遷移します。
- ② 「オプション」メニューから「リンク切れ検知設定」をクリックします。
- ③ 「リンク切れ検知設定」画面で「有効」を選択し、「設定する」ボタンをクリックします。

リストの表示方法

リンク切れ検知設定を有効にし、次回の解析以降、「リンク切れ検知リスト」が表示されます。

管理コンソール TOP 画面の下部にある「リンク切れ検知リスト」ボタンをクリック。
リンク切れを検知したリスト一覧ページにジャンプします。

The screenshot shows a dashboard with a dark blue header labeled "Dashboard". Below the header, there are several widgets:

- 最終結果** (Final Result): Shows a date and time "2022年5月13日 21:48" and a "SAFE" status with a green shield icon.
- 直近の解析結果** (Recent Analysis Results): A bar chart showing six bars for dates: 12/24 21:48, 12/24 21:48, 1/21 21:48, 2/18 21:48, 3/18 21:48, 4/16 21:48, 5/13 21:48.
- ウィークリーの解析結果** (Weekly Analysis Results): A bar chart showing six bars for weekly periods: 12/19~12/25, 1/16~1/22, 2/13~2/19, 3/13~3/19, 4/10~4/16, 5/8~5/14.
- マンスリーの解析結果** (Monthly Analysis Results): A bar chart showing six bars for months: 2021/12, 2022/1, 2022/2, 2022/3, 2022/4, 今月.
- 本日の解析結果履歴** (Today's Analysis Results History): A section with the text "本日の解析結果はまだありません" (No analysis results for today). It contains three buttons: "解析URLのリストをダウンロード" (Download list of analysis URLs), "リンク構造を見る" (View link structure), and "リンク切れ検知リスト" (Link break detection list). The "リンク切れ検知リスト" button is highlighted with a red box and a red arrow points to it from the right.

リンク切れ検知リスト https://[redacted] 監視中

リンクが切れているURLは以下です。

全 6件

URL	操作
https://[redacted]99992.html	リンク切れ箇所を見る
https://[redacted]	
詳細 404:404 - Not Found	
https://[redacted]99999.html	リンク切れ箇所を見る
https://[redacted]99998.html	リンク切れ箇所を見る
https://[redacted]ken1.html	リンク切れ箇所を見る

「+」ボタンをクリックすると詳細情報を表示します。

- . . . リンク切れの URL
- . . . リンク切れの URL がリンクされている URL

詳細 . . . サーバからの応答エラーコード

リンク切れ箇所を見る . . . リンク構造の可視化ページにジャンプします（「6.7 リンク構造可視化機能」参照）

6.7 リンク構造可視化機能

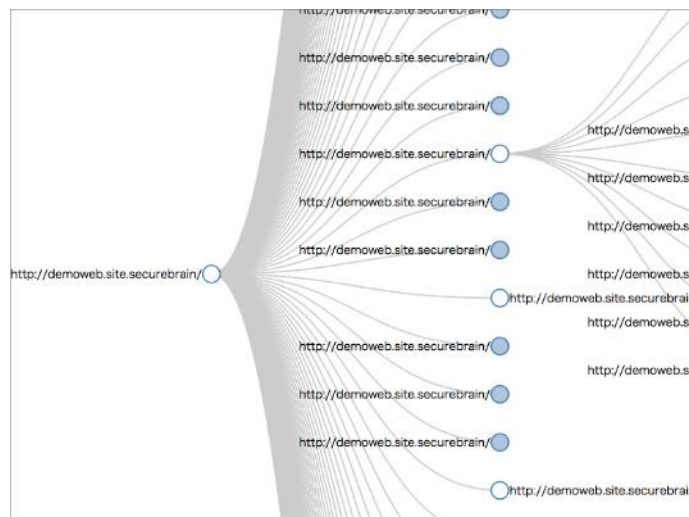
リンク構造可視化機能（以下、本機能）は、GREd のクローラが改ざんの有無を検査するために収集した情報を元にサイトのリンク構造をツリー状に表示し可視化します。本機能を使用し改ざん検知箇所やアラート検知箇所、またリンク切れ検知箇所等を視覚的に理解していただくことで、影響範囲の把握や復旧の迅速化にお役立ていただけます。

リンク構造の表示方法

管理コンソール TOP 画面の下部にある「リンク構造を見る」ボタンをクリック。リンク構造の可視化ページにジャンプします。



TOP ページからリンクしているページをツリー状に表示します。



リンク構造のツリーはマウスで拡大・縮小・移動が可能です。

● をクリックするとそのページにリンクされているページ一覧が表示されます。

○ 表示の場合は、そのページにリンクされているページがありません。

改ざん・クロスドメイン等を検知した場合の表示



「検知箇所を表示」ボタンをクリックすると検知箇所がツリーの中心に表示されます。改ざん検知した URL は赤色に変わります。クロスドメイン、表層解析等を検知した URL はオレンジに変わります。どちらの場合でも、URL の先頭のマルが赤になり点滅します。検知箇所が複数ある場合は、緑の右矢印ボタンをクリックするとトップ URL に近い順に表示されます。

リンク構造の表示は改ざん箇所や内容を通知する詳細レポートからも可能です。管理コンソール TOP 画面のカレンダーのアイコンをクリックし、詳細レポートから「検知箇所を見る」をクリックしてください。

注意が必要です

2022年5月16日 10:47



リンク切れを検知した場合の表示

管理コンソール TOP 画面の下部にある「リンク切れ検知」ボタンをクリック。
 リンク切れを検知したリスト一覧ページにジャンプします。

The screenshot shows the 'Dashboard' interface. It includes several widgets:

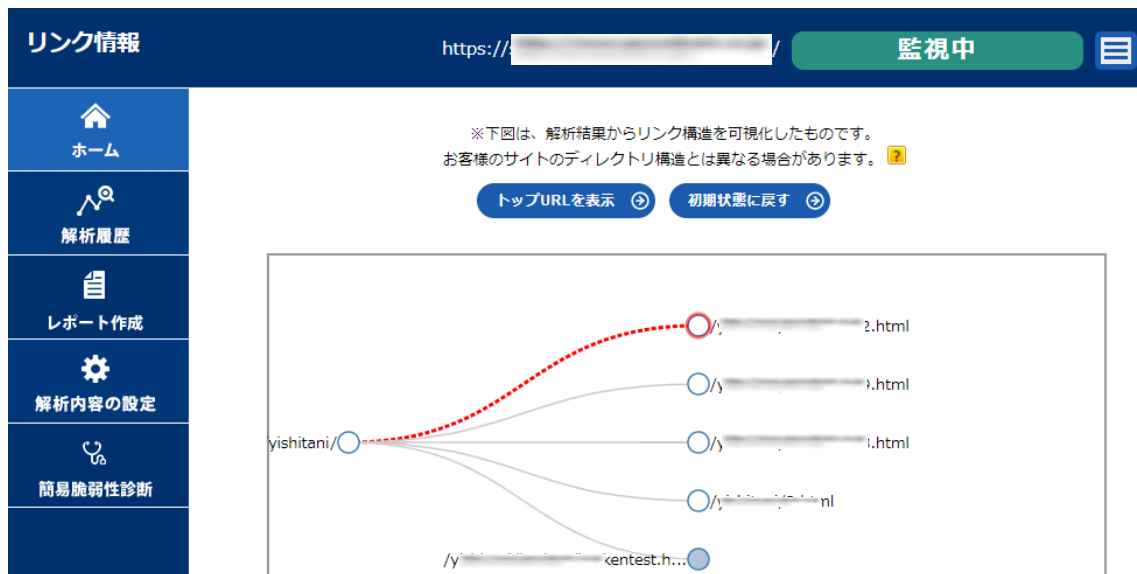
- 最終結果** (Final Result): Shows a 'SAFE' status for the scan on 2022年5月13日 21:48.
- 直近の解析結果** (Recent Analysis Results): A bar chart showing analysis results for dates from 12/24 to 5/13.
- ウィークリーの解析結果** (Weekly Analysis Results): A bar chart showing analysis results for weekly periods from 12/19 to 5/8.
- マンスリーの解析結果** (Monthly Analysis Results): A bar chart showing analysis results for months from 2021/12 to the current month.
- 本日の解析結果履歴** (Today's Analysis Result History): A section indicating that no results are available for today. It contains three buttons: '解析URLのリストをダウンロード', 'リンク構造を見る', and 'リンク切れ検知リスト'. The 'リンク切れ検知リスト' button is highlighted with a red box and a red arrow pointing to it.

The screenshot shows the 'リンク切れ検知リスト' (Broken Link Detection List) page. The page title is 'リンク切れ検知リスト' and the status is '監視中' (Monitoring). The page content includes:

- A message: 'リンクが切れているURLは以下です。' (The following URLs are broken links.)
- A count: '全 6件' (Total 6 items).
- A table of broken links with columns for 'URL' and 'リンク切れ箇所を見る' (View broken link location). The table lists several URLs, including 'https://s...99992.html', 'https://s...99999.html', 'https://s...99998.html', and 'https://...ken1.html'. The 'リンク切れ箇所を見る' button for the last entry is highlighted with a red box and a red arrow pointing to it.

「リンク切れ箇所を見る」をクリックするとリンク構造の可視化ページにジャンプします。

リンク切れの部分は赤の点線で表示されます。リンク切れ URL の先頭のマルが赤になり点滅します。



リンク構造のツリーはマウスで拡大・縮小・移動が可能です。

●をクリックするとそのページにリンクされているページ一覧が表示されます。

○表示の場合は、そのページにリンクされているページがありません。

対応ブラウザ

Edge, Chrome, Firefox

【ご注意事項】

- ・本機能で表示されるリンク構造は、GREED の解析結果からリンク構造を可視化したものです。お客様のサイトのディレクトリ構造とは異なる場合があります。
- ・管理コンソール TOP 画面のカレンダーからリンク構造を可視化できる期間は、直近1週間です。
- ・可視化処理は JavaScript で動作しているため、処理時間はお使いの PC のスペックに依存します。

【免責事項】

利用者は自らの責任及び判断において本機能を利用するものとし、直接的・間接的を問わず 利用者が本機能を利用したことにより生じたあらゆる損害、損失、責任、負担に対して 当社は一切責任を負わないものとします。

6.8 全サイトの状態

複数スケジュールを登録している場合、複数スケジュールの直近 1 ヶ月の解析情報を表示します。

※複数スケジュールが無い場合は、「全サイトの状態」ボタンは表示されません。
ヘッダーの「全サイト操作」の「直近一か月の解析結果」からアクセスできます。

全サイト操作 ▼ ユーザー情報 ログアウト

全サイト

直近一か月の解析結果 ①

一括ダウンロード

クロスドメイン共通許可リスト

最新の解析結果

改ざんを発見しました 20.0%

安全です 40.0%

注意が必要です 40.0%

②

直近一か月の検知情報(悪質 / 警告)

表示件数 10件 ▼

1-3 件目 (全 3件)

解析サイト	解析結果	検知日時
[Redacted]	注意が必要です	2024年02月22日 11時50分
[Redacted]	注意が必要です	2024年02月22日 11時49分
[Redacted]	改ざんを発見しました	2024年02月22日 11時49分

1-3 件目 (全 3件)

③

	項目名	内容
①	直近一か月の解析結果	全サイトの状態を表示します。
②	最新の解析結果	全スケジュールの最新の解析結果を円グラフで表示します。(緑色：正常、黄色：クロスドメインスクリプトの検知、赤色：改ざんの検知)
③	直近一か月の検知 (悪質/警告)	1 ヶ月以内の検知 (悪質/警告) した、解析サイト名と、URL を表示します。

6.9 一括ダウンロード

複数スケジュールを登録している場合、複数スケジュールの解析 URL リストとレポートを一括ダウンロードできます。

※複数スケジュールが無い場合は、「一括ダウンロード」ボタンは表示されません。
ヘッダーの「全サイト操作」の「一括ダウンロード」からアクセスできます。

Web 改ざんチェック Cloud 全サイト操作 ユーザー情報 ログアウト

一括ダウンロード

直近一カ月の解析結果

一括ダウンロード ①

クロスドメイン共通許可リスト

スケジュールの絞り込み

解析URLのリストとレポートの一括ダウンロードを行います。絞り込む条件を指定してください。

検索するタイトル

検索するURL

最新の解析結果

すべて 成功 失敗 警告 未解析

絞り込む

結果一覧 | 一括操作

表示件数 10件

1-2 件目 (全 2件)

全てチェック(ページ内)

<input type="checkbox"/>	解析サイト	監視	結果
<input type="checkbox"/>	テストサイト2	ON	成功
<input type="checkbox"/>	テストサイト1	ON	失敗

1-2 件目 (全 2件)

URLリストのダウンロード

ダウンロード

レポートのダウンロード

月次

2022年05月

ダウンロード

日次

2022年5月16日

ダウンロード

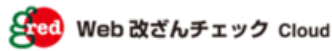
※解析履歴の保存期間は1年間です

戻る

	項目名	内容
①	一括ダウンロード	一括ダウンロード画面に遷移します。
②	スケジュールの絞り込み	複数スケジュールを条件により絞り込みます。
③	スケジュール一覧	スケジュール検索結果の一覧を表示します。 チェックボックスをチェックすることで、URL リストのダウンロード、レポートのダウンロードを行うスケジュールを選択出来ます。
④	URL リストのダウンロード	③で選択したスケジュールの、最新の解析履歴 URL リストをダウンロードします。 リストファイルと、インデックスファイルが ZIP 形式でダウンロード出来ます。
⑤	レポートのダウンロード 月次	③で選択したスケジュールの、月次 (指定月一ヵ月分) レポートをダウンロードします。 レポート対象の年月を指定し、CSV ファイルでダウンロード出来ます。
⑥	レポートのダウンロード 日次	③で選択したスケジュールの、日次 (指定日一日分) レポートをダウンロードします。 レポート対象の年月日を指定し、CSV ファイルでダウンロード出来ます。

6.10 パスワードをお忘れの場合

パスワードをお忘れによりログインできない場合に、ログインフォームの下にある『パスワードをお忘れの場合』リンクからパスワードを再設定することができます。あわせて二要素認証の設定を無効化することもできます。



6.11 ログイン履歴確認機能

これまでのログイン日時とそのログインを行った環境の IP を表示します。1 ページに最大 100 件が表示され、最長で過去 1 年分のログイン履歴を表示することができます。

ログイン履歴

⚠ ログイン履歴の表示期間は最長1年です。

ログイン日時	ログインIPアドレス
2022年07月15日 15:31:47	██████████
2022年07月15日 14:11:27	██████████
2022年07月15日 13:42:53	██████████
2022年07月14日 16:33:35	██████████
2022年07月14日 16:29:09	██████████
2022年07月14日 16:28:41	██████████

7. 申込み（新規申込・変更申請）

7.11 新規申込

所定の申込書にホスト名（FQDN：解析開始 URL）と解析 URL 数、お客様情報をご記入の上、提出してください。標準プランは、1 ホスト、1000URL、1 日 4 回解析になります。

標準プラン以外をご希望の場合は、購入元の代理店にご相談ください。

新規申込が完了すると GREED システムから申し込み時に指定していただいたアラートメールアドレスに登録通知が届きます。

※所定の申込書は、巻末の「付録 新規申込/解約申請書」をご参照ください。

※管理画面の URL の詳細は、巻末の「付録 管理画面 URL」をご参照ください。

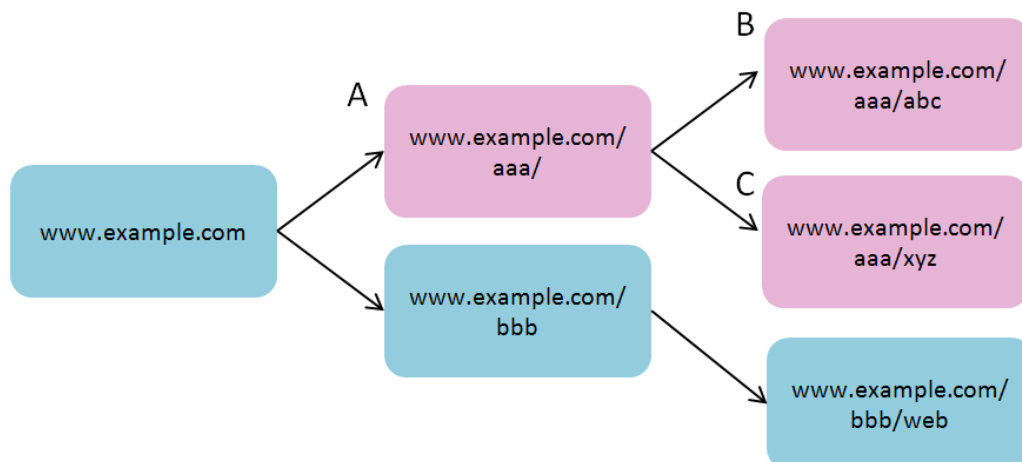
7.12 解析する URL 数、解析対象ホスト数

「GREED Web 改ざんチェック Cloud」の価格は、解析する URL 数、解析の対象とするホスト数によって変わります。まず、お客様の Web サイトの URL 数をご確認ください。URL 数が不明な場合は、購入元の代理店でカウントすることも可能ですので、お問い合わせください。

7.13 解析する URL の絞り込み(除外 URL の登録)

除外 URL の設定が可能です。解析 URL 数を調節する際にお使いいただけます。パス（ディレクトリ）指定を最大 100 個まで行うことができます。この機能は、指定したパス（ディレクトリ）以降をチェックしません。（この機能は、契約後、お客様が管理コンソールから設定します。設定方法は、「5.4 除外 URL の登録」をご覧ください。）

※A(www.example.com/aaa/)を指定した場合、B と C も解析対象から除外されます。



7.14 解析する URL の絞り込み(ウェブ解析対象階層の指定)

解析対象の階層数を指定する事により、不要なページのスキャンを防止いたします。指定された階層以降はページが存在していても解析を行わず、解析対象ページ数としてもカウントいたしません。(この機能は、契約後、お客様が管理コンソールから設定します。設定方法は、「5.6 監視の ON/OFF とウェブ解析対象階層の指定」をご覧ください。)

7.15 変更申請

所定の変更申請書に変更内容をご記入の上、提出してください。

※所定の変更申請書は、巻末の「付録 変更申請書」をご参照ください。

付録 新規申込書

お客様にて、赤枠内をご記入ください。

お申し込みいただく前に、GREd Web改ざんチェック Cloudをご利用いただくための契約条件 (<https://www.gred.jp/saas/other/agreement.html>) をよくお読みください。お客様が本サービス申込みをいただいた時点で、これらの条項に同意されたものとみなさせていただきますようお願い申し上げます。

弊社は、お客様からご提供いただく個人情報、弊社のプライバシーポリシー (<https://www.hitachi-systems.com/privacy/index.html>) を遵守した上で、弊社が企画・後援するイベントやセミナー、新製品のご案内をはじめとする営業・マーケティング活動に利用する場合がございますので予めご了承くださいようお願い申し上げます。

GREd Web改ざんチェック Cloud 新規申請書

*1 希望日有りの場合: 希望日の5営業日前迄に提出、最遅希望日「最遅」と明記。

[1] 申請内容 ※赤枠部分は、記入必須項目です。 本申請書の提出が遅れた際は、ご希望日に添えない場合がございます。▼

お申し込み日	20 年 月 日	サービス開始希望日 *1	20 年 月 日
契約種別 (年額/月額/月額自動更新*2)	選択してください	基本契約数(基本ライセンス)	1ホスト・1,000URL
解析回数(基本:1日4回)	1日4回	ホスト追加ライセンス <small>追加購入された数字を入力*</small>	0 ライセンス
ユーザID (ログインID)*3		合計ホスト数 <small>入力不可*</small>	1 ホスト
アラート用メールアドレス*4・5		URL数追加ライセンス <small>追加購入された数字を入力*</small>	0 ライセンス
管理画面利用ご担当者名*6		合計URL数 *7 <small>入力不可*</small>	1,000 URL

【サービス解約ご希望の場合】 解約希望月の1ヶ月前までに別途、解約申請書にて申請が必要となります。なお、料金の日割り計算は出来ないので、月中であっても解約利用月分の料金は発生しますのでご了承ください。解約申請書が必要な際は、パートナーセールス(partner_sales@securebrain.co.jp)までご連絡下さい。

*1: サービス開始日は、営業日の関係上、前倒しもしくは翌月のサービス開始日になる場合があります。納期につきましてはご販売会社へお問い合わせ下さい。

*2: 【月額自動更新について】 月額サービスはお客様が解約を1ヶ月前までに申請されない限り、自動継続として更新されます。

*3: ログインで使用するIDです。ユーザID(ログインID)は登録後、変更はできません。その為個人アドレスはお勧めしません。使用可能な文字は0~50文字の半角英数字と、ダッシュ(-)、アンダースコア(_)、スラッシュ(/)、ピリオド(.)、アットマーク(@)です。

*4: 関連メール(サービス開始と管理画面のログイン情報のお知らせ)、並びに、改ざん発見時のアラートメール送信先となります。メールアドレスを1つご記入下さい。

*5: 【サービス開始後のアラート用メールアドレス・管理画面利用ご担当者名の変更ご希望の方】 お客様管理画面(<https://www.gred.jp/saas/>)へログインいただき、「ユーザー情報の変更」からご自身の変更をお願いしております。尚、弊社へ変更連絡は不要です。もし、現在のアラート用メールアドレスの登録情報をご退職者様のアドレス等の理由により受信出来ず、管理画面でログイン出来ない場合には、サポートセンター(E-mail: biz_support@securebrain.co.jp)>(<https://www.securebrain.co.jp/support/index.html>)へ連絡して下さい。ご希望のアドレスへ変更致します。

[2] ホスト(解析開始URL)とURL数

ホスト(解析開始URL) *8		URL数
※必ず https:// (又はhttp://) からご記入をお願いします。		
No.	(記入例) https://www.securebrain.co.jp	(例) 1000
(1)		
(2)		
(3)		
(4)		
(5)		
(6)		
(7)		
(8)		
(9)		
(10)		
合計URL数(セルM12参照) 入力不可*		0
*7: 複数のホストがある場合は、「合計URL数」内に納まるように、数を割り当ててください。		

*8-1: ドメインが同一の場合でも、サブドメインが異なる場合は別ホストとなりますので、ご注意ください。(例)「www.securebrain.co.jp」と「info.securebrain.co.jp」は、別ホスト扱い。

*8-2: FQDNが同一の場合でも、解析開始URLが異なる場合は別ホスト扱いとなりますので、その分のライセンスの追加が必要になります。(例) 「<https://www.securebrain.co.jp/>」と「<https://www.securebrain.co.jp/eng/>」は、別ホスト扱い。

[3] お客様情報 ◎契約者が管理画面利用者も兼ねられる場合は、管理画面利用者の欄には「同左」とご記入いただいても結構です。

	ご契約者 (サービスの購入と管理をされる方)	管理画面利用者 (GREdシステムを利用し、サポートを受けられる方)
■会社名		
■ご所属部署/役職名		
■ご担当者名		こちらの利用者は、上方記載*8と同一の方となります。担当者名・メールアドレスの変更方法は*8を参照下さい。尚、グレー部分の変更につきましては、弊社への変更連絡は不要でございます。
■電子メールアドレス		
■電話番号		
■備考	ご契約者と管理画面利用者とは別に、エンドユーザーがある場合は、エンドユーザー名をご記載下さい	

[4] パートナー情報

	パートナー(販売1次店)	パートナーの代理店(販売2次店)
■会社名		
■ご所属部署/役職名		
■ご担当者名		
■電子メールアドレス*9 (更新案内連絡先)		社名以外、申請不要
■電話番号		
■備考	注文番号(PO番号)等、必要に応じてご記入下さい	

*9: 月額自動更新以外は、更新案内メールの送信にも利用させていただきますので、案内メールの受取先メールアドレスをご連絡ください。3アドレスまで可。

SBC(20231211)

付録 変更申請書

GREd Web改ざんチェック Cloud 変更申請書

弊社は、お客様からご提供いただく個人情報を、弊社のプライバシーポリシー(https://www.hitachi-systems.com/privacy/index.html)を遵守した上で、弊社が企画・後援するイベントやセミナー、新製品のご案内をはじめとする営業・マーケティング活動に利用する場合がございますので予めご了承くださいようお願い申し上げます。

[1]サービス内容 ▼下記条件、ご記入ください。

お申し込み日	年 月 日	基本ライセンス(1ホスト・1000URL)	変更前	変更後
変更希望日*3	年 月 日	ホスト追加ライセンス <small>追加購入された数字を入力</small>	0	0
契約種別 <small>(年額/月額/月額自動更新)</small>	選択ください	合計ホスト数 <small>入力不可、自動計算</small>	1	1
ユーザID (ログインID) <small>*1: ユーザIDは変更できません。</small>		URL追加ライセンス <small>追加購入された数字を入力</small>	0	0
アラートメールアドレス*2(任意)		合計URL数 *4 <small>入力不可、自動計算</small>	1,000	1,000
管理画面利用 ご担当者名*2(任意)		解析回数(基本:1日4回)	要選択	要選択

*2: 項目を変更方法「管理画面(https://www.gred.jp/saas/)へログイン後「ユーザー情報の変更」から、お客様ご自身で変更をお願い致します。尚、弊社への変更連絡は不要です。
もし、現在のアラート用メールアドレスの登録情報をご退職者様のアドレス等の理由により受信出来ず、管理画面にログイン出来ない場合には、サポートセンター(E-mail: biz_support@securebrain.co.jp>https://www.securebrain.co.jp/support/index.html)へ連絡して下さい。ご希望のアドレスへ変更致します。

*3: 希望日有りの場合: 希望日の5営業日前迄に提出。最速希望の場合: 「最速」と明記下さい。内容に不備がある場合、再提出等、受理する迄にリードタイムを要する為、余裕をもって申請下さい。

[2]ホスト(解析開始URL)とURL数の設定 *5

*5-1. ホスト(解析開始URL)は必ずhttps://(又はhttp://)からご記入下さい。	▼「区分*6」を選択して下さい。
*5-2. 改ざん時切り替え機能をご利用の場合、開始URLを変更される場合は、変更後のページに改ざん時切り替え機能のタグを挿入して下さい。	変更 ・解析開始URLの変更の場合: 上書き変更され、解析履歴は引き継がれます。 ・URL数の増減の場合: ご希望のURL数を明記下さい。
*5-3. ドメインが同一の場合でも、サブドメインが異なる場合は、別ホスト扱いとなりますので、追加ライセンスが必要になります。 (例) [www.securebrain.co.jp]と[info.securebrain.co.jp]は、別ホスト扱い。	追加(ホスト) ・新たなホストNoに、解析開始URL明記下さい。「新規ホスト」として追加します。 ※削除依頼したホストNo欄に追記はご遠慮下さい。
*5-4. FQDNが同一の場合でも、解析開始URLが異なる場合は、別ホスト扱いとなりますので、その分のライセンスの追加が必要になります。 (例) [https://www.securebrain.co.jp/]と[https://www.securebrain.co.jp/eng/]は、別ホスト扱い。	変更無 ・対応無し。 ※変更前URLをそのまま、変更後欄へ明記下さい。 削除 ・変更希望日(当日)、又は5営業日以内に削除されます。 【削除依頼時の注意】 ・行削除・結めて明記はせず、「削除」選択下さい。左右対称でなくなる為。 ・URLの削除後は、解析履歴の閲覧が出来なくなる為、もし履歴が必要な際は、変更希望日前迄に管理画面の「解析履歴」より事前DLをお願い致します。

【重要: 課金月について】日割り計算は行っていない為、通常、下記の通りです。
・ホスト数やURL数を減少する場合は、**翌月より減額**
・ホスト数やURL数を追加する場合は、**当月より増額**
※上記対応が難しく、日程や課金調整が必要な場合はお問合せ下さい。

変更前				変更後			
ホストNo.	ホスト(解析開始URL) *5	URL数	区分 *6	ホスト(解析開始URL) *5	URL数	合計ホスト数	合計URL数 *4: セル「08」参照 複数ホストの場合、「合計URL数」内で割振り下さい
1			要選択			0	0
2			要選択			0	0
3			要選択			0	0
4			要選択			0	0
5			要選択			0	0
6			要選択			0	0
7			要選択			0	0
8			要選択			0	0
9			要選択			0	0
10			要選択			0	0
合計ホスト数	0	合計URL数 *4: セル「08」参照 複数ホストの場合、「合計URL数」内で割振り下さい		合計ホスト数	0	合計URL数 *4: セル「08」参照 複数ホストの場合、「合計URL数」内で割振り下さい	0

[3]お客様・[4]パートナー情報に変更がある場合、変更されたい部分のみ、ご記入ください。

▼変更箇所チェック	ご契約者 (サービスの購入と管理をされる方)	管理画面利用者 (GREdシステムを利用し、サポートを受けられる方)
<input type="checkbox"/> 会社名 <input type="checkbox"/> ご所属部署/役職名 <input type="checkbox"/> ご担当者名 <input type="checkbox"/> 電子メールアドレス <input type="checkbox"/> 電話番号 備考: ご契約者と管理画面利用者とは別に、エンドユーザーがある場合は、E/URL名をご記載下さい		こちらの利用者は、上記記載*2と同一の方となります。 担当者名・メールアドレスの変更方法は*2を参照下さい。 尚、グレー部分の変更におきましては、弊社への変更連絡は不要でございます。
▼変更箇所チェック	パートナー(販売1次店)	パートナーの代理店(販売2次店)
<input type="checkbox"/> 会社名 <input type="checkbox"/> ご所属部署/役職名 <input type="checkbox"/> ご担当者名 <input type="checkbox"/> 電子メールアドレス*6 (更新案内連絡先) <input type="checkbox"/> 電話番号 備考: 注文番号(PO番号)等、必要に応じてご記入下さい		社名以外、申請不要

*6: 月額自動更新以外は、更新案内メールの送信にも利用させていただきますので、案内メールの受取先メールアドレスをご連絡ください。3アドレスまで可。

SBG(20231211)

付録 解約申請書

お申し込みいただく前に、GREd Web改ざんチェック Cloudをご利用いただくための契約条件(<https://www.gred.jp/saas/other/agreement.html>) をよくお読みください。
お客様が本サービス申込みをいただいた時点で、これらの条項に同意されたものとみなさせていただきますのでご了承くださいませようお願い申し上げます。

弊社は、お客様からご提供いただく個人情報を、弊社のプライバシーポリシー(<https://www.hitachi-systems.com/privacy/index.html>)を遵守した上で、弊社が企画・後援するイベントやセミナー、新製品のご案内をはじめとする営業・マーケティング活動に利用する場合がございますので予めご了承くださいませようお願い申し上げます。

GREd Web改ざんチェック Cloud 解約申請書

[1]申請内容 ※赤枠内を埋めていただきますようお願い致します。

解約申請日*1	20 年 月 日	サービス解約希望月*2 (最終課金月)	20 年 月
解約理由 今後のサービス向上に役立てる為、お聞かせいただけますと幸いです。			

*1: 解約希望月の1ヶ月前までに申請が必要となります。

*2: 解約希望月の翌月第1営業日に、解約のお手続き(サービス停止)させていただきます。
(例)解約希望月:2022年10月の場合、2022年11月1日に解約処理となります。
月途中の解約をご希望の方は、日にも茲ご記入ください。解約希望日で停止をさせていただきます。
尚、解約日が月途中でも、料金の日割り計算は出来ませんのでご了承ください。
稀に年末年始・GW等、弊社都合で作業が遅れることもございますが、課金は解約月迄となりますのでご安心下さい。
もし遅れる場合、作業日については、内容を確認後、担当者よりご連絡いたします。

[2]現在ご提供中のサービス内容*3

ユーザID (ログインID)	
アラート用メールアドレス(任意)	
管理画面利用 ご担当者名(任意)	

*3: URLの解析履歴に関しましては、解析日時から1年経過したURLごとに、自動で削除されます。
履歴を残したい場合には、管理画面の「解析履歴」より、ダウンロードをお願い致します。

[3]お客様情報 ◎ご契約者が管理画面利用者も兼ねられる場合は、管理画面利用者の欄には「同左」とご記入いただいても結構です。

	ご契約者 (サービスの購入と管理をされる方)	管理画面利用者 (GREdシステムを利用し、サポートを受けられる方)
■会社名		
■備考	ご契約者と管理画面利用者とは別に、エンドユーザーがある場合は、エンドユーザー名をご記載下さい。	

[4]パートナー情報

	パートナー(販売1次店)	パートナーの代理店(販売2次店)
■会社名		
■備考		

この度は、弊社サービスをご利用いただき、誠にありがとうございました。
今後とも、サービスの向上に努めてまいりますので、また機会がございましたら株式会社セキュアブレインをよろしくお願いたします。

SBC(20231211)

付録 管理画面 URL

管理画面 URL は以下の通りです。

管理画面 URL	https://www.gred.jp/saas/
----------	---

付録 アラートメールサンプル

アラート通知メールのサンプルは以下の通りです。

1	改ざん検知時
2	Top ページのヘルスチェック 検知時
3	見た目変化検知時
4	クロスドメインスクリプト検知時
5	EXE 解析検知時
6	タグ変化検知時/JavaScript 変化検知時
7	週間レポート
8	お知らせ通知

1. 改ざん検知時

送信元	gred@service.securebrain.co.jp
件名	[GREd]Web 改ざんの可能性を検知
本文サンプル	<p>「GREd Web 改ざんチェック」からのお知らせです。</p> <p>監視中の Web ページに Web 改ざんの可能性を発見しました。</p> <p>Web 改ざんが発見された URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。改ざんを検知した Web ページの詳細確認は、必ず下記の Web サイトからご確認下さい。</p> <p>_____</p> <p>監視中の Web サイト： _____</p> <p>検知 URL： _____</p> <p>内容：脆弱性を持つサイトの疑いのあるコンテンツが発見されました</p> <p>このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。</p>

3. 見た目変化検知時

送 信 元	gred@service.securebrain.co.jp
件 名	[GREd]TOP ページの見た目が変化した可能性を検知
本 文	<p>「GREd Web 改ざんチェック」からのお知らせです。</p> <p>監視中の Web サイトで TOP ページの見た目が変化した可能性を検知しました。</p> <p>TOP ページの見た目の変化を検知した URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 Web ページの詳細は、必ず下記の Web サイトからご確認ください。</p> <p style="background-color: #e0f0ff; padding: 5px; margin: 10px 0;">[Redacted]</p> <p>監視中の Web サイト： [Redacted]</p> <p>検知 URL： [Redacted]</p> <p>内容：見た目変化の可能性の疑いのあるコンテンツが発見されました</p> <p style="margin-top: 20px;">このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除してください。 本メールは、送信専用メールアドレスからお送りしています。</p>

4. クロスドメインスクリプト検知時

送 信 元	gred@service.securebrain.co.jp
件 名	[GREd]クロスドメインスクリプトを検知
本 文	<p>「GREd Web 改ざんチェック」からのお知らせです。</p> <p>監視中の Web ページに新たなドメインから実行する下記のクロスドメインスクリプトを発見しました。</p> <p>このスクリプトが正規に追加されたスクリプトの場合は必ず、[解析内容の設定]-[クロスドメイン設定]-[クロスドメイン検知]の設定画面：「許可リスト」にクロスドメインの登録を行ってください。</p> <p>Web 改ざんが発見された URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。 改ざんを検知した Web ページの詳細確認は、必ず下記の Web サイトからご確認下さい。</p> <p style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;">[Redacted]</p> <p>監視中の Web サイト： [Redacted]</p> <p>検知 URL： [Redacted]</p> <p>内容：クロスドメインスクリプトの疑いのあるコンテンツが発見されました</p> <p>検知経路： [Redacted]</p> <p style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;">[Redacted]</p> <p>このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。</p>

5. EXE 解析検知時

送信元	gred@service.securebrain.co.jp
件名	[GREd]ファイルのマルウェア類似挙動の可能性を検知
本文	<p>「GREd Web 改ざんチェック」からのお知らせです。</p> <p>監視中の Web ページにリンクされたファイルのマルウェア類似挙動の可能性を検知しました。</p> <p>マルウェア類似挙動の可能性を検知した URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。Web ページの詳細は、必ず下記の Web サイトからご確認ください。</p> <p>_____</p> <p>監視中の Web サイト： _____</p> <p>検知 URL： _____</p> <p>内容：怪しいファイルの疑いのあるコンテンツが発見されました</p> <p>この検知はマルウェアとして検知するものではなく、あくまでもマルウェア類似の動きを検知したものです。検知したファイルが正常なものである場合、ホワイトリストに登録することで以降の検知を回避することができます。ホワイトリストに登録するかどうかは、自社にて判断ください。</p> <p>このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除してください。本メールは、送信専用メールアドレスからお送りしています。</p>

6. タグ変化検知時/JavaScript 変化検知時

送 信 元	gred@service.securebrain.co.jp
件 名	[GREd]Web コンテンツデータが変化した可能性を検知
本 文	<p>「GREd Web 改ざんチェック」からのお知らせです。</p> <p>監視中の Web ページで Web コンテンツデータが変化した可能性を検知しました。</p> <p>Web コンテンツデータの変化を検知した URL をブラウザで直接アクセスするとマルウェアに感染する可能性があります。Web ページの詳細は、必ず下記の Web サイトからご確認ください。</p> <p style="text-align: center;">[Redacted]</p> <p>監視中の Web サイト： [Redacted]</p> <p>検知 URL： [Redacted]</p> <p>内容：スクリプト/リンクタグ変化の疑いのあるコンテンツが発見されました</p> <p>このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除してください。 本メールは、送信専用メールアドレスからお送りしています。</p>

7. 週間レポート

送 信 元	gred@service.securebrain.co.jp
件 名	[GREd]週間レポート
本 文	<p>_____様、</p> <p>いつもGREdの「Web改ざんチェック」サービスをご利用いただきましてありがとうございます。 本サービスはWeb改ざんを検知し、迅速な対応を可能にするセキュリティサービスです。</p> <p>今週のレポートを送付させていただきます。</p> <p>----- 今週のWeb改ざんチェックのレポート -----</p> <p>レポート期間： _____</p> <p>監視中のWebサイト： _____</p> <p>対象ドメイン：</p> <p>1週間でチェックした回数：2回</p> <p>改ざんを通知した回数：0回</p> <p>警告を通知した回数：1回</p> <p>貴社のWebページ数(平均)：3ページ</p> <p>-----</p> <p>詳細な情報や、週間レポート送信サービスの設定を変更する場合は、gred セキュリティサービスにログインして「ユーザ情報の変更」で行ってください。 https://www.gred.jp/saas/</p> <p>このメールにお心当たりのない方は、リンクをクリックせず、このメールを削除して下さい。 本メールは、送信専用メールアドレスからお送りしています。</p>

8. お知らせ通知

送信元	gred@service.securebrain.co.jp
件名	GREd Web 改ざんチェックからのお知らせ 【\${CATEGORY}】
本文	<p>【 ██████████ 】 ██████████</p> <p>██████████</p> <p>ログイン画面 URL : ██████████</p> <p>本メールは、送信専用メールアドレスからお送りしています。</p> <p>=====</p> <p>GREd Web 改ざんチェック</p> <p>Web 改ざんを検知し、迅速な対応を可能にするセキュリティサービス</p> <p>-----</p>

通知メールの件名の\${CATEGORY}は、お知らせの種別により変わります。

- 重要なお知らせ : システムメンテナンス等のお知らせメールの場合
- ご案内 : 新機能の追加等の案内メールの場合
- 障害 : 障害が発生時の通知メールの場合